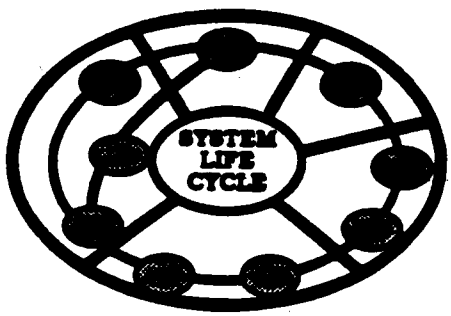
OFFICE OF SOLID WASTE AND EMERGENCY RESPONSE (OSWER)



SYSTEM LIFE CYCLE MANAGEMENT GUIDANCE

Part 3: Practice Paper

Application Security Management During the System Life Cycle

October 1991

Practice Paper: Application Security Management During the System Life Cycle

Table of Contents

LIST OF EXHIBITS

PRACTICE PAPER : APPLICATION SECURITY MANAGEMENT DURING THE SYSTEM LIFE CYCLE

Chapter 1

INTRODUCTION

1.1 Practice Paper Purpose

This practice paper provides details to *project managers* concerning their responsibilities for Application Security Management for both new applications and existing applications under the Office of Solid Waste and Emergency Response (OSWER) System Life Cycle Management Guidance. This practice paper describes application security management throughout the application *life cycle*, and provides guidance concerning *objectives, key decisions, activities, products* and *baselines* that the *project manager* must address from *Initiation* through *Archive*.

This practice paper has three primary purposes:

- Focus each *project manager's* attention on application security management
- Facilitate appropriate application security management for each OSWER application
- Provide a common *approach* to application security management across OSWER

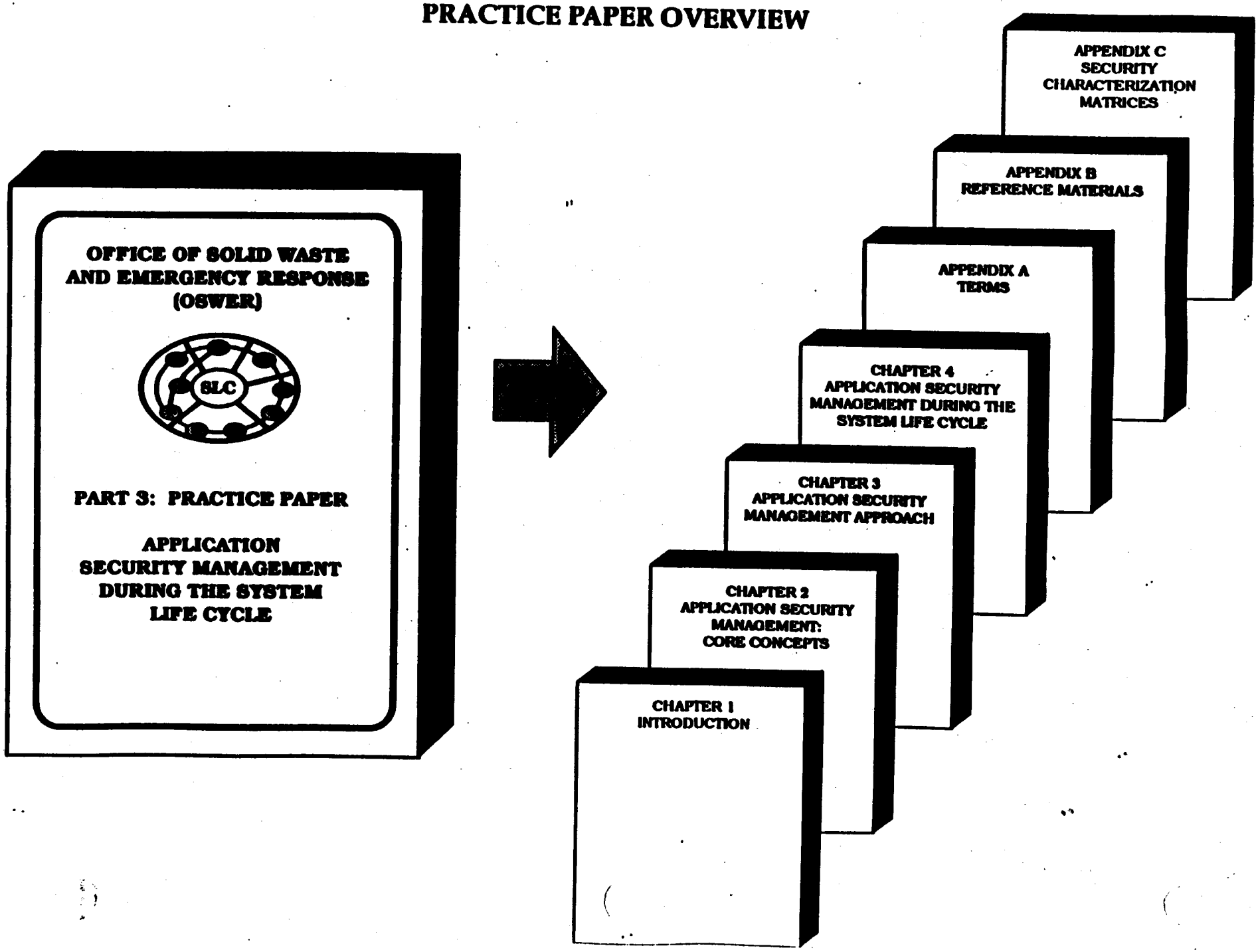
This practice paper constitutes a section of Part 3 of the OSWER System Life Cycle Management Guidance.

1.2 Practice Paper Topics

Exhibit 1-1 provides an overview of the structure of this practice paper. Topics addressed are:

- An introduction to core application security concepts
- Selection of an application security management *approach* for both new and existing applications
- Consideration of application security management *objectives, key decisions, activities, products,* and *baselines* at each *life cycle phase* and *stage*

EXH .T 1-1
APPLICATION SECURITY MANAGEMENT PRACTICE PAPER OVERVIEW



The following notation is used:

- *Terms* which have special meaning in relationship to the OSWER System Life Cycle Management Guidance appear in small italic letters.
- *CORE CONCEPTS*, described in Chapter 2, appear in capital letter italics.

1.3 Application Security Management Responsibilities

Project Managers are responsible for implementing this guidance for new or existing OSWER applications. Specifically, they are responsible for selecting an application security management *approach*, documenting the *approach* in the *Project Management Plan*, and ensuring that this *approach* is implemented throughout the *life cycle*.

Application *data stewards*, *custodians*, and *users* are responsible for carrying out all relevant agency security guidance and *SECURITY MEASURES* which are to be implemented for the application.

1.4 Basic Principles

The following basic principles provide the foundation for all OSWER application security management *objectives*, *key decisions*, *activities*, *products* and *baselines*:

- Application security management is critical to the effective and efficient accomplishment of OSWER's programmatic mission.
- Application security management is an integral component of every *phase* and *stage* of the *life cycle*.
- All OSWER applications are *SENSITIVE* to some degree.
- Application security management involves *data stewards*, *custodians*, and *users* as well as *project managers*, developers and maintainers.
- Application security management is a continuing and dynamic process.
- Application security management involves not only the application itself, but also the installations and facilities where the application is developed and operated, along with the personnel who develop and operate it.

1.5 Why Focus Upon Application Security Management?

This practice paper focuses on application security management throughout the *life cycle* for the following reasons:

- Application security management is a relatively new discipline. Because of this, it is often poorly understood by application system *project managers, data stewards, custodians* and *users*.

- Many *THREATS* and the *VULNERABILITIES* these *THREATS* exploit are so subtle that they are easily overlooked.

- Many *ADVERSE EVENTS* occur so rarely that they are seldom considered even though the magnitude of harm or *RISK* is relatively great.

- Computer-based application systems are often more *VULNERABLE* to loss of *AVAILABILITY, INTEGRITY, CONFIDENTIALITY* and to *INAPPROPRIATE USE* than the manual systems they replace.

- Retrofitting *SECURITY MEASURES* into an operational application is often more costly and less effective than integrating or coordinating them with other *activities* throughout the application *life cycle*.

- A number of Federal oversight agencies, as well as EPA, have issued policies and directives regarding application security management. OSWER needs to be assured that their application systems comply with these policies and directives.

1.6 How to Use this Practice Paper

Before reading Chapters 2 through 4 of this practice paper, be sure to read Part 2 of the OSWER System Life Cycle Management Guidance. In addition, pay special attention to the practice papers on "System Life Cycle Reviews and Approvals," "Benefit-Cost Analysis," "Data Management During the System Life Cycle," "Configuration Management," and the *"Project Management Plan"* which are in Part 3. You will also need to reference the "EPA Information Security Manual."

Use Chapter 2 to familiarize yourself with the core concepts of application security management. You will need a thorough understanding of these concepts before you develop your application security management *approach*. Chapter 3 describes the essential components of your *approach*. Consult Chapter 4 as you actually develop and refine your *approach* throughout the *life cycle*.

Be sure to take advantage of the Appendices. Appendix A not only defines important terms, but cross-references them to numerous oversight agency policies and directives. Appendix B contains an annotated bibliography of oversight agency policies and directives as well as other important reference material. The Security Characterization Matrices in Appendix C provide concrete examples of material which is discussed on a more theoretical level in Chapters 2 and 4. The "Guidelines For Security of Computer Applications" (FIPS PUB 73) as well as the "EPA Information Security Manual," were used in the formulation of these matrices.

1.7 Topics Not Addressed in this Practice Paper

This practice paper is designed to complement OSWER's System Life Cycle Management Guidance. Because of this, it is more focused than most other material on application security management. For example, configuration management and data quality (i.e., accuracy, precision, completeness, and consistency) are often considered to be security issues. However, as they are covered elsewhere in the Guidance, they are not included here.

Additionally, this practice paper does not contain guidance on how to conduct a security *RISK ANALYSIS*. *RISK ANALYSIS* is a specialized subject on which much excellent reference material is readily available.

Nor does this practice paper contain recommendations for the implementation of specific *SECURITY MEASURES* unless they have been specifically required by federal oversight or agency guidance. This is because *SECURITY MEASURES* should not be selected until a *RISK ANALYSIS* has been conducted and a determination made of appropriateness and cost effectiveness. Again, a great deal of good material has been written on this subject.

Chapter 2

APPLICATION SECURITY MANAGEMENT: CORE CONCEPTS

2.1 Introduction

The purpose of this chapter is to introduce you to a number of core application security management concepts. You will need to understand these concepts in order to develop your application security management *approach*.

2.2 Core Concepts

2.2.1 OSWER's Security Objectives: Availability, Integrity, Confidentiality and Appropriate Use

OSWER has four *APPLICATION SECURITY OBJECTIVES*. The first three are explicitly mandated by the Computer Security Act of 1987, external oversight guidance and the agency's security policy. These three *APPLICATION SECURITY OBJECTIVES* are *AVAILABILITY, INTEGRITY*, and *CONFIDENTIALITY*. OSWER has added a fourth *OBJECTIVE* to this list. That *OBJECTIVE*, implicit, but not directly expressed in our oversight guidance, is *APPROPRIATE USE* of our *INFORMATION RESOURCES*.

Each of these *SECURITY OBJECTIVES* is defined as follows:

- *AVAILABILITY*: OSWER develops applications to support our programmatic mission. The loss of *AVAILABILITY* of any *INFORMATION RESOURCE* associated with an application could affect the application's ability to support some aspect of the mission. *AVAILABILITY* refers to having our applications ready and able to support our programmatic mission at the time they are needed.

- *INTEGRITY*: All *INFORMATION RESOURCE* components of an application must retain the functionality they were designed to have in order to support the programmatic mission. *INFORMATION RESOURCES* have *INTEGRITY* as long as their functionality remains uncompromised, that is, they must do no more, no less than their intended purpose.

- *CONFIDENTIALITY*: Some OSWER applications contain data or provide information which during a specified period of time is not subject to the Freedom of Information Act and must not be disclosed without authorization. *CONFIDENTIALITY* refers to our need to have certain of our data and information held in confidence.

- *APPROPRIATE USE/INAPPROPRIATE USE:* While *INAPPROPRIATE USE* or misuse of an application may not result in direct loss of *AVAILABILITY, INTEGRITY,* or *CONFIDENTIALITY,* misuse of our *INFORMATION RESOURCES* is clearly undesirable and sometimes unlawful. In OSWER we want to ensure that our applications are used for, and only for, support of our programmatic mission.

2.2.2 Sensitivity/Sensitive

All OSWER applications are *SENSITIVE* to some degree: this is because, to some extent, they are *VULNERABLE* to loss of *AVAILABILITY* and/or *INTEGRITY,* to *INAPPROPRIATE USE* and some to loss of *CONFIDENTIALITY.* However, there are different degrees of *SENSITIVITY* depending on the relevance of OSWER's *SECURITY OBJECTIVES* to the information management problem to be solved. For example, *AVAILABILITY* might be very relevant to a mission critical application; *INTEGRITY* to a decision support application, and *CONFIDENTIALITY* to an application processing confidential business information. It follows that the greater the relevancy, the greater the degree of *SENSITIVITY.*

Note that data and information can also be considered *SENSITIVE,* as defined in Appendix A.

2.2.3 Information Resources

OSWER applications involve data, information, hardware, software, documentation, facilities, telecommunications and trained staff. These components of each application are our *INFORMATION RESOURCES.* All *INFORMATION RESOURCES* have value in and of themselves. Equipment costs money to acquire, replace or repair. Staff costs money to hire, retain and train. Software costs money to develop and maintain. However, the ultimate value of our *INFORMATION RESOURCES* are the support they provide to our programmatic mission.

2.2.4 Adverse Event

In the broadest sense, the loss of an application's *AVAILABILITY, INTEGRITY, CONFIDENTIALITY* or *INAPPROPRIATE USE* are *ADVERSE EVENTS.* Anything that adversely affects any application *INFORMATION RESOURCE* is also an *ADVERSE EVENT* since this in turn results in loss of *AVAILABILITY, INTEGRITY, CONFIDENTIALITY* or takes additional resources to replace or recover.

For example, malfunctioning equipment could result in loss of *AVAILABILITY.* A change in an application's software could result in a loss of *INTEGRITY.*

Inadvertent disclosure of enforcement *SENSITIVE* information could result in a loss of *CONFIDENTIALITY*. *INAPPROPRIATE USE*, such as violating software licensing agreements or copyrights, is an *ADVERSE EVENT* since it could expose the agency to legal complications. Refer to the matrix on *ADVERSE EVENTS* in Appendix C for more examples.

2.2.5 Threat

A *THREAT* is anything that can cause an *ADVERSE EVENT*. Every application is faced with countless *THREATS*. For the sake of simplicity, however, they can be thought of as just two basic types: people and change to the environment. People can deliberately or inadvertently cause *ADVERSE EVENTS*. For example, deliberate acts by people result in *ADVERSE EVENTS* such as loss of *AVAILABILITY* through malicious destruction of *INFORMATION RESOURCES* or loss of *INTEGRITY* through fraudulent manipulation of *INFORMATION RESOURCES*. Inadvertent acts by people, like leaving *SENSITIVE* information on a screen, could result in loss of *CONFIDENTIALITY*. Unexpected or unwanted change such as flood, fire, smoke, dust, or power loss, could result in similar *ADVERSE EVENTS*. Even anticipated change can be a problem: think about the last time you had to adjust to a new operating system or to an upgrade of your PC software.

THREATS can be as obvious as an earthquake or as subtle as a virus. They can change throughout an application's *life cycle*, and frequently do so. For a logically organized matrix of common *THREATS* and how they relate to our *SECURITY OBJECTIVES* in different processing environments see Appendix C.

2.2.6 Vulnerability

Where there is a chance that a *THREAT* can reach an *INFORMATION RESOURCE* and cause an *ADVERSE EVENT* there is *VULNERABILITY*. Identifying and communicating *VULNERABILITY* can be quite challenging. While some *VULNERABILITIES* are immediately obvious (e.g., a password posted on the wall), others may be much more technical or subtle (e.g., spaghetti code). In general, you can assume that the more complex, distributed, and widely used your application, the more *VULNERABLE* it is.

Also like *THREATS*, *VULNERABILITIES* can change throughout an application's *life cycle*. See Appendix C for a matrix organized by *VULNERABILITIES* to each *INFORMATION RESOURCE* and how they relate to our *SECURITY OBJECTIVES* in different processing environments.

2.2.7 Risk

Technically, *RISK*, also termed "loss expectancy," is the predicted loss from an *ADVERSE EVENT* during a certain period of time. Risk is often expressed in terms of dollars and cents, but not always. The period of time is usually expressed in years, but not necessarily so. For example, the *RISK* of having to reenter transactions which were lost due to hardware failure could be $5 per update cycle. The *RISK* of having to pay prompt payment penalties due to a software error in an accounts payable program could be $25,000 per year. Non-monetary *RISKS* are sometimes expressed in terms such as inconvenience, delay and loss of credibility.

Also like *THREATS* and *VULNERABILITIES*, *RISKS* change throughout the application's *life cycle* and require frequent evaluation.

2.2.8 Risk Analysis

The methodology to determine *RISK* by analyzing potential *ADVERSE EVENTS*, *THREATS*, and *VULNERABILITIES* against *INFORMATION RESOURCES*, as well as the likelihood of occurrence, is called *RISK ANALYSIS*. *RISK ANALYSES* are either qualitative or quantitative. They may be conducted at a very summary level, in great detail, or somewhere in between.

A detailed quantitative *RISK ANALYSIS*, is a highly specialized technical task, not to be undertaken lightly. However, there is a great deal of good reference material on various methodologies for conducting *RISK ANALYSES*. See Appendix B for citations. The "EPA Information Security Manual" and "Guideline for Automatic Data Processing Risk Analysis" (FIPS PUB 65) also provide guidance on conducting qualitative *RISK ANALYSIS*.

2.2.9 Security Measures

SECURITY MEASURES counter or control *THREATS*. By definition, when an appropriate *SECURITY MEASURE* is in place and being used effectively, *VULNERABILITY* is reduced. However, keep in mind, there is no perfect world, at least where application security is involved. An appropriate *SECURITY MEASURE* is not always available. And even when they are available, *SECURITY MEASURES* are not always in place. As a result, no application is ever completely *VULNERABILITY* free.

SECURITY MEASURES are often categorized by their purpose. These purposes are prevention, detection, minimization, and recovery. For example:

- Cipher locks prevent unauthorized entry

- Audit trails detect fraud
- Training minimizes user errors
- Frequent data backup aids recovery.

Since every application is always *VULNERABLE* to some extent, minimization and recovery *SECURITY MEASURES* take on added importance. For example, separation of duties ensures that exposure is minimized even if misuse occurs. Also, contingency planning (for applications) or continuity of operations planning (for installations) for recovery from *ADVERSE EVENTS* ranging from mild disruptions to *AVAILABILITY* to all-out disasters needs to be part of every application's repertoire of *SECURITY MEASURES*.

SECURITY MEASURES can also be categorized by their type and subtype. For federal government security planning purposes, the Office of Management and Budget (OMB) has categorized *SECURITY MEASURES* as management controls, development controls, operational controls, security awareness and training, technical controls, and support system controls. These categories, and the subcategories under them, have been based on numerous Government Accounting Office (GAO) and National Institute of Standards and Technology (NIST) guidance.

A more traditional categorization of types of *SECURITY MEASURES*, and the one used in this practice paper, is physical, technical, administrative, and managerial. Keyboard locks are a physical *SECURITY MEASURE*. Implementing software access protection, such as Resource Access Control Facility (RACF), is a technical *SECURITY MEASURE*. Maintaining a list of authorized users is an administrative *SECURITY MEASURE*. Developing an application security management *approach* and documenting it in the *Project Management Plan* is a managerial *SECURITY MEASURE*.

It is also important to understand that there is not always a one-to-one relationship between *THREATS* and *SECURITY MEASURES*. One *THREAT* may be countered by a number of *SECURITY MEASURES*. For example, bans on smoking, smoke detectors, equipment covers, and fire extinguishers are all effective *SECURITY MEASURES* for fire. On the other hand, many *THREATS* may be countered by one *SECURITY MEASURE*. Off-site back ups are an effective *SECURITY MEASURE* against numerous unwanted or unanticipated changes as well as inadvertent and deliberate acts by people.

Another thing to keep in mind is that not all *SECURITY MEASURES* are perfectly compatible. By countering one *THREAT* they may make another *THREAT* more likely. For example, ceiling fire extinguishers may cause water damage as they douse the fire. Labeling confidential printouts or diskettes "sensitive," to indicate special handling, may draw unwanted attention.

And finally, with just one exception, *SECURITY MEASURES* are never completely free. Some *SECURITY MEASURES*, such as hardware encryption devices, may cost thousands of dollars. Even *SECURITY MEASURES* such as passwords have cost implications in terms of increased internal processing time and decreased user access efficiency. Fortunately, some *SECURITY MEASURES*, are automatically derived from following OSWER System Life Cycle Management Guidance for Data Management, Configuration Management, testing, etc. and reduce *VULNERABILITY* at no additional cost. The same holds true for compliance with guidance already required by agency property management and personnel management policy. The one exception, the *SECURITY MEASURE* which is completely free, and probably the ultimate in protection, is a suspicious mind! Never, ever underestimate its value.

See Appendix C for a matrix of common *SECURITY MEASURES* by purpose, *SECURITY OBJECTIVE*, typical processing environment, and applicable *phase* and *stage*.

2.2.10 Benefit Cost-Analysis

Benefit-cost analysis is a systematic approach for comparing alternative ways to satisfy an objective. Benefit-cost analyses are conducted throughout the OSWER *life cycle*. The benefits to be realized through *RISK* reduction as well as the costs to develop, acquire, implement, operate, periodically evaluate and eventually archive *SECURITY MEASURES* need to be considered along with all other application benefits and costs.

Be sure to reference the OSWER System Life Cycle Management Guidance practice paper on *Benefit-Cost Analysis*. In addition, Appendix C of the "EPA Information Security Manual" and "Guidance for Automatic Data Processing Risk Analysis" (FIPS PUB 65) provide guidance on identifying RISKS and selecting appropriate *SECURITY MEASURES*.

Chapter 3

APPLICATION SECURITY MANAGEMENT APPROACH

3.1 Introduction

This chapter provides guidance on developing and refining your application security management *approach*, for either new or existing applications, throughout the *life cycle*.

3.2 What is an Application Security Management Approach?

An application security management *approach* is only one facet of your overall *project management approach*. It focuses on ensuring that OSWER's *SECURITY OBJECTIVES* of *AVAILABILITY, INTEGRITY,CONFIDENTIALITY* and *APPROPRIATE USE* are met throughout an application's *life cycle*. An application security management *approach* addresses security management specific *objectives, key decisions, activities, products* and *baselines* at every *phase* and *stage*. The rigor and formalism of your *approach* should reflect the degree of *SENSITIVITY* of the application.

3.3 Why Choose An Application Security Management Approach?

An application security management *approach* is necessary to ensure that OSWER's *SECURITY OBJECTIVES* are effectively met and that they are met in a cost efficient manner. Too often, security is addressed as an afterthought resulting in ineffective and inefficient retrofitted *SECURITY MEASURES*. In contrast, *SECURITY MEASURES*, well integrated within the application, throughout the *life cycle*, can greatly enhance an application's overall effectiveness and efficiency. Ultimately, good application security management is the most important and effective *SECURITY MEASURE*.

3.4 Special Considerations for Roles and Responsibilities

Because security is a specialized technical area, requiring both empirical and theoretical knowledge, you may need to give special consideration to the assignment of roles and responsibilities. Your project team may need to include experts in *RISK ANALYSIS*, hardware and software *SECURITY MEASURES*, technical writing, and security training. Some applications may require assistance in areas such as the Freedom of Information Act and Privacy Act procedures and the

agency's confidential business information (CBI) processes. In some cases you will need to consult auditors from the Office of the Inspector General and you may want to have them working with you from *Initiation* through *Implementation* and for periodic *Evaluations*. During the *Production stage*, substantial security responsibilities may be placed on your application *data stewards, custodians*, and primary and secondary *users*. *Users*, in particular, tend not to be security oriented and will often need special training and frequent re-enforcement in order to fulfill their security roles and responsibilities.

The "EPA Information Security Manual" contains further material on roles and responsibilities.

3.5 Determining and Documenting Your Application Security Management Approach

The *life cycle* development and refinement of your application security management *approach* is an iterative process. As you progress through each *phase* and *stage*, your *approach* will become more focused and detailed.

You will summarize your overall application security management *approach* for *Program Management* in each of the *Decision Papers*. You will document the details of your *approach* in the *Project Management Plan*. At the end of each *life cycle phase* and *stage* before entering a new one, your *Project Management Plan* should document your application security management *approach* by describing the *objectives* met, and the "why," "who," "what," "where," "when," and "costs" of each *key decision* made, *activity* completed, *product* delivered and *baseline* added or updated during the just completed *phase or stage*. At the same time, the *Plan* should address your *workplan* for the next *phase* or *stage*.

You may choose to organize all your application security *approach* documentation under a "Security Management Approach" heading in the *Project Management Plan*, or to place it under other topic headings. For example, the details on application security roles and responsibilities could appear under "Project Team Organization." Security training and awareness could appear under "User Support Approach" while the cost for *SECURITY MEASURES* could be included in the "Project Budget."

Be sure to take advantage of the wealth of reference materials readily available to you. Start with the EPA Headquarters Library since they have an excellent information resources management (IRM) collection. See Appendix B for a list of reference materials which include a selection of security videos available from the Washington Information Center (WIC). Also, don't neglect to consider software tools available to you for *RISK ANALYSIS* and *benefit-cost analysis*.

Chapter 4

APPLICATION SECURITY MANAGEMENT DURING THE SYSTEM LIFE CYCLE

4.1 Introduction

The OSWER System Life Cycle Management Guidance includes some references to application security in various *products* such as the *System Concept, Detailed Functional Requirements, Detailed Data Requirements,* and *System Design.* In contrast, the purpose of this chapter is to specifically address your dynamically evolving application security management *approach* at each *phase* and *stage* of the OSWER *life cycle* for both new and existing applications. It provides the information you, as a *project manager,* need to develop your *approach* and to document this *approach* in the various *Decision Papers* and your *Project Management Plan.* It also provides information you need to comply with various EPA and federal requirements regarding application security management.

As is described in Part 2 of the Guidance, your *approach* involves identifying the project *objectives* and the "why," "who," "what," "where," "when," and "costs," of *key decisions, activities, products* and *baselines* as they relate to application security management for each *phase* and *stage* listed below:

Phases	Stages
Initiation	Initiation
Concept	Concept
Definition and Design	Definition Design
Development and Implementation	Development Implementation
Operation	Production Evaluation Archive

There are many issues which complicate application security management. This chapter attempts to show the multifaceted nature of application security management. It does not recommend or discuss specific *SECURITY MEASURES* (except by way of example), but rather provides a structured methodology for introducing *SECURITY MEASURES* appropriate to the application at the correct

phase or *stage*. The remainder of this chapter is divided into sections corresponding to each *life cycle phase* and *stage*. For each *phase* and *stage*, the following is covered:

- Brief description of the results of the previous *phase* or *stage* and summary of work to be conducted during this *phase* or *stage*
- Guidelines for conducting each application security management *activity*
- Special considerations for developmental *SECURITY MEASURES*
- Descriptions of key *products* and *baselines*, including documents required by various oversight organizations, highlighted in Exhibit 4.1-1
- Graphic summary of *objectives, key decisions, activities, products* and *baselines*

4.2 Application Security Management During the Initiation Phase

4.2.1 Overview

During the *Initiation phase* you select an overall application security management *approach* which reflects the *SENSITIVITY* of your application.[1] This *approach* will be further refined throughout the remainder of the *life cycle*. You also develop a detailed *approach* for the *Initiation phase* which addresses application security-related project *objectives, key decisions, activities,* and *products* as well as the creation of the *Initiation baseline*. See Exhibit 4.2-1 for an overview of these topics.

By the end of the *Initiation phase*, you will have:

- Determined the degree of *SENSITIVITY* of your application
- Performed an order-of-magnitude *benefit-cost analysis*
- Determined what *SECURITY MEASURES* need to be in place for the *Concept phase*

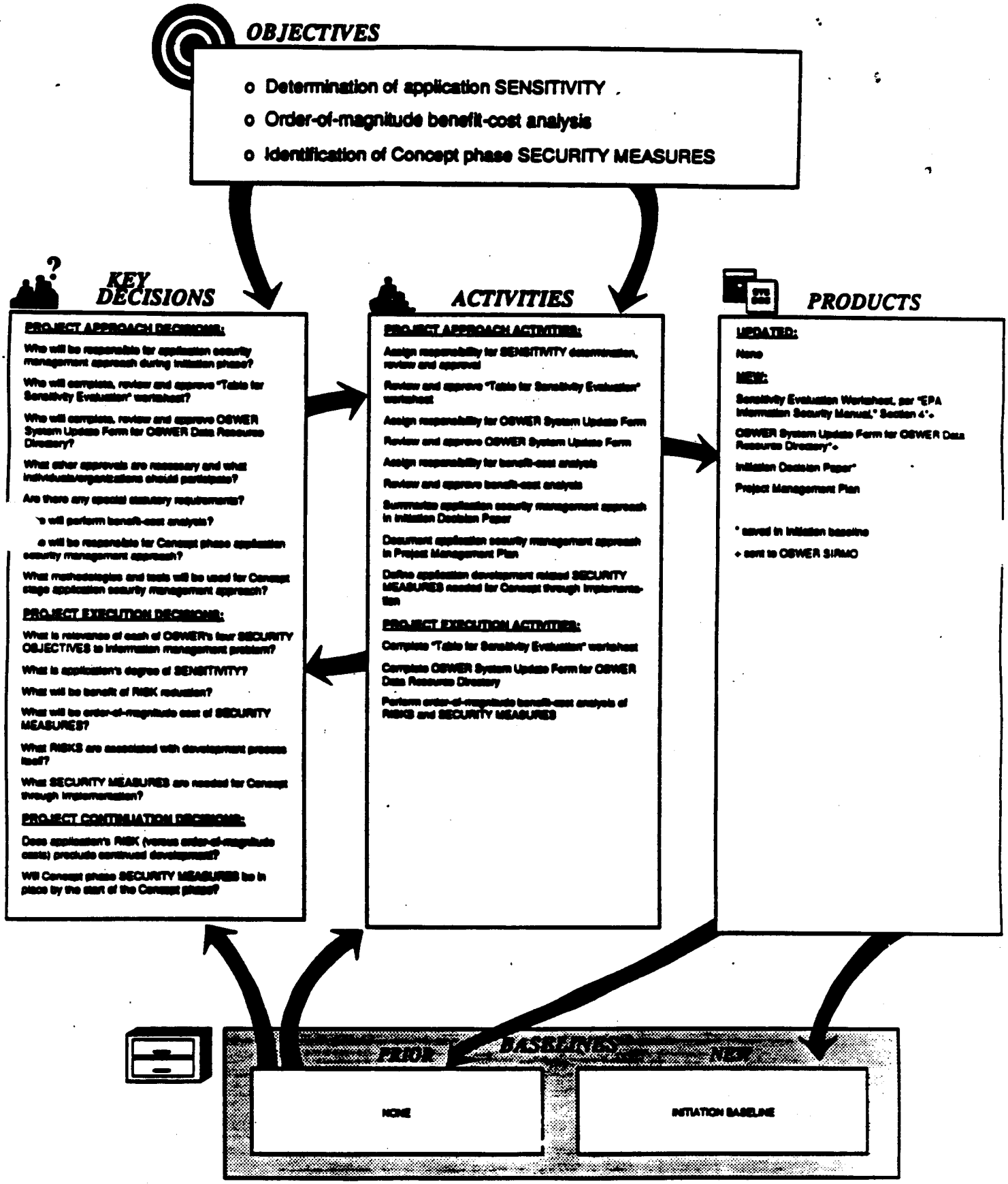
[1]The term "application" is used generically here since the decision on whether or not automation is an appropriate solution to the information management problem will not be made until the *CONCEPT* phase.

Exhibit 4.1-1 Oversight Organization Documentation Requirements

Document	OSWER Life Cycle Phase/Stage									Comment
	Init.	Con.	Def.	Des.	Dev.	Impl.	Prod.	Eval.	Arch.	
Table for Sensitivity Evaluation (EPA Manual, Section 4)	IN							UN	A	Management Approval; Submit to SIRMO for Annual Report to OIRM
OSWER System Update Form	IN		U					UC	A	Submit to SIRMO for OSWER Data Resource Directory
NIST/NSA Security Plan (OMB Bulletin 90-08)				IN		UN		U1	A	Submit to SIRMO
Qual. Risk Analysis Worksheet (EPA Manual, Appendix C)				IN				U5 UC	A	Submit to SIRMO for Annual Report to OIRM
Quant. Risk Analysis Report (EPA Manual, Appendix C)				IN				U5 UC	A	Submit to SIRMO for Annual Report to OIRM
Continuity/Contingency Plan (EPA Manual, Appendix D)					IN			UC	A	Submit to SIRMO for Annual Report to OIRM
Security Manual (or other operational doc.)					IN	UN		UN	A	Submit to SIRMO for Annual Report to OIRM
Security Training Statement						IN	U1		A	Submit to SIRMO for Annual Report to OIRM
Appl. Certification Worksheet (EPA Manual, Appendix B)						IN		IE U3 UC	A	Submit to SIRMO for Annual Report to OIRM

Legend: IN = initial submission for new systems; IE = initial submission for existing systems
U = update; UN = update as needed
U1 = update annnually
U3 = update every three years
U5 = update every five years
UC = update upon significant change
A = archived

EXHIBIT 4.2-1: INITIATION PHASE
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



4.2.2 Initiation Phase Activities

4.2.2.1 Sensitivity Determination

Your first *activity* is determining your application's relative *SENSITIVITY* (e.g., high, medium or low). This determination of *SENSITIVITY* is basic to the development of your application security management *approach* and will come in to play again and again in many ways throughout the *life cycle*. Highly *SENSITIVE* applications require formal, detailed, well documented approaches, while applications with low *SENSITIVITY* require only the implementation of the minimal *SECURITY MEASURES* prescribed in the "EPA Information Security Manual."

To determine *SENSITIVITY* you follow the three step methodology provided in Chapter 4 of the "EPA Information Security Manual." The methodology includes completing a worksheet called the "Table for Sensitivity Evaluation." You should note that you <u>may</u> determine your application to be <u>more</u> *SENSITIVE* than the worksheet indicates. For example, if your application contains Confidential Business Information (CBI), you might consider *CONFIDENTIALITY* to be highly relevant to your information management problem (rather than medium as Table 4-2 suggests) and therefore your application to be highly *SENSITIVE*. However, you may <u>not</u> determine your application to be <u>less</u> *SENSITIVE* than indicated by the agency's methodology.

You should also note that the worksheet addresses only *AVAILABILITY*, *INTEGRITY*, and *CONFIDENTIALITY*. The fourth OSWER *SECURITY OBJECTIVE*, *APPROPRIATE USE*, must be considered also. Add your determination of relative *SENSITIVITY* to *APPROPRIATE USE* as an addendum to the worksheet.

You also document the degree of SENSITIVITY on the OSWER System Update Form.

4.2.2.2 Order-of-Magnitude Benefit-Cost Analysis

The OSWER System Life Cycle Management Guidance requires you to conduct an order-of-magnitude *benefit-cost analysis* during the *Initiation phase*, as described in the practice paper on *benefit-cost analysis* in Part 3 of the Guidance. Obviously, you need to balance the benefits of *RISK* reduction against the costs of the *SECURITY MEASURES* needed throughout the *life cycle*. At this early *phase* in the *life cycle*, you will have to settle for high level assumptions. As a general rule, the higher the *SENSITIVITY*, the greater the benefits from *RISK* reduction. On the other hand, the greater the complexity and the larger and more dispersed the user community, the greater the costs for *SECURITY MEASURES*.

4.2.3 Special Considerations for Developmental Security Measures During the Initiation Phase

During *Initiation*, you also need to consider what *RISKS* are associated with the application development process itself. For example, if you were developing an invoice payment application, you might need to implement *SECURITY MEASURES* during *Definition, Design, Development,* and *Implementation* to prevent an embezzler from altering your software as it is being defined, designed, coded, tested, or installed. As another example, you might need *SECURITY MEASURES* to prevent unauthorized disclosure of your *Security Manual* as it is being written, edited, or distributed. You may need personnel screening throughout the *life cycle.* Appendix C will help in identifying *THREATS* and *SECURITY MEASURES* applicable to the development process.

4.2.4 Initiation Phase Products and Baselines

Table for Sensitivity Evaluation

You complete this worksheet as described above in Section 4.2.2.1. You must have the "Table for Sensitivity Evaluation" worksheet approved by the appropriate manager as designated in the *Project Management Plan.* Once approved, add it to the *Initiation baseline* and submit it to the OSWER Senior Information Resource Management Officer (SIRMO) for reporting in OSWER's annual security report to the Office of Information Resources Management (OIRM).

OSWER System Update Form

Once you have completed the *SENSITIVITY* determination you can complete the *SECURITY MEASURES* section of the OSWER System Update form for the OSWER Data Resource Directory. This form is initially submitted to the OSWER Senior Information Resource Management Officer (SIRMO) at the completion of the *Initiation phase.* It is also included in the *Initiation baseline.*

Initiation Decision Paper

At the end of the *Initiation phase,* you summarize your overall application security management *approach* for the entire *life cycle* in the *Initiation Decision Paper.* Be sure to address your rationale for determining the degree of *SENSITIVITY* and the order-of-magnitude cost of *SECURITY MEASURES* over the course of the entire *life cycle.*

Project Management Plan

You document your overall application security management *approach* in the *Project Management Plan.* Your *approach* should address your project *objectives, key decisions, activities, products* and *baselines.* Be sure to include:

- Any special application security requirements (e.g., Privacy Act, confidential business information (CBI))
- Identification of the elements of the project management structure that relate to application security management *activities,* particularly individuals responsible for reviewing and approving *Initiation phase products* and *baselines.,* using the "EPA Information Security Manual" for guidance as to appropriate roles and responsibilities
- Description of the methodology used for *SENSITIVITY* determination
- Benefits to be derived from *RISK* reduction
- Order-of-magnitude cost estimate for *SECURITY MEASURES,* including developmental *SECURITY MEASURES*
- Plans for acquiring, implementing, operating, evaluating and eventual archiving of *SECURITY MEASURES* for the *Concept phase* through *Operation phase*

You also need to develop and document an application security management *approach* workplan for the *Concept phase.* It should cover new *objectives, key decisions, activities, products* and *baselines.* Be sure to address:

- *SECURITY MEASURES* needed to be in place before the *Concept phase* begins
- Proposed methodology for *Concept phase activities*
- *Concept phase activities,* as defined in Section 4.3

Refer to the topical outline for the *Project Management Plan* given in Part 2 of the OSWER System Life Cycle Management Guidance for the *Initiation phase.*

4.3 Application Security Management During the Concept Phase

4.3.1 Overview

You selected your overall application security management *approach* during the *Initiation phase*. Your *approach* was based on a determination of the relative *SENSITIVITY* of your application. You also conducted an order-of-magnitude *benefit-cost analysis* of *RISK* reduction benefits versus *SECURITY MEASURE* costs.

During the *Concept phase* your detailed application security management *approach* addresses new application security-related project *objectives, key decisions, activities* and *products*, as well as the updated *Initiation baseline*. See Exhibit 4.3-1 for an overview of these topics.

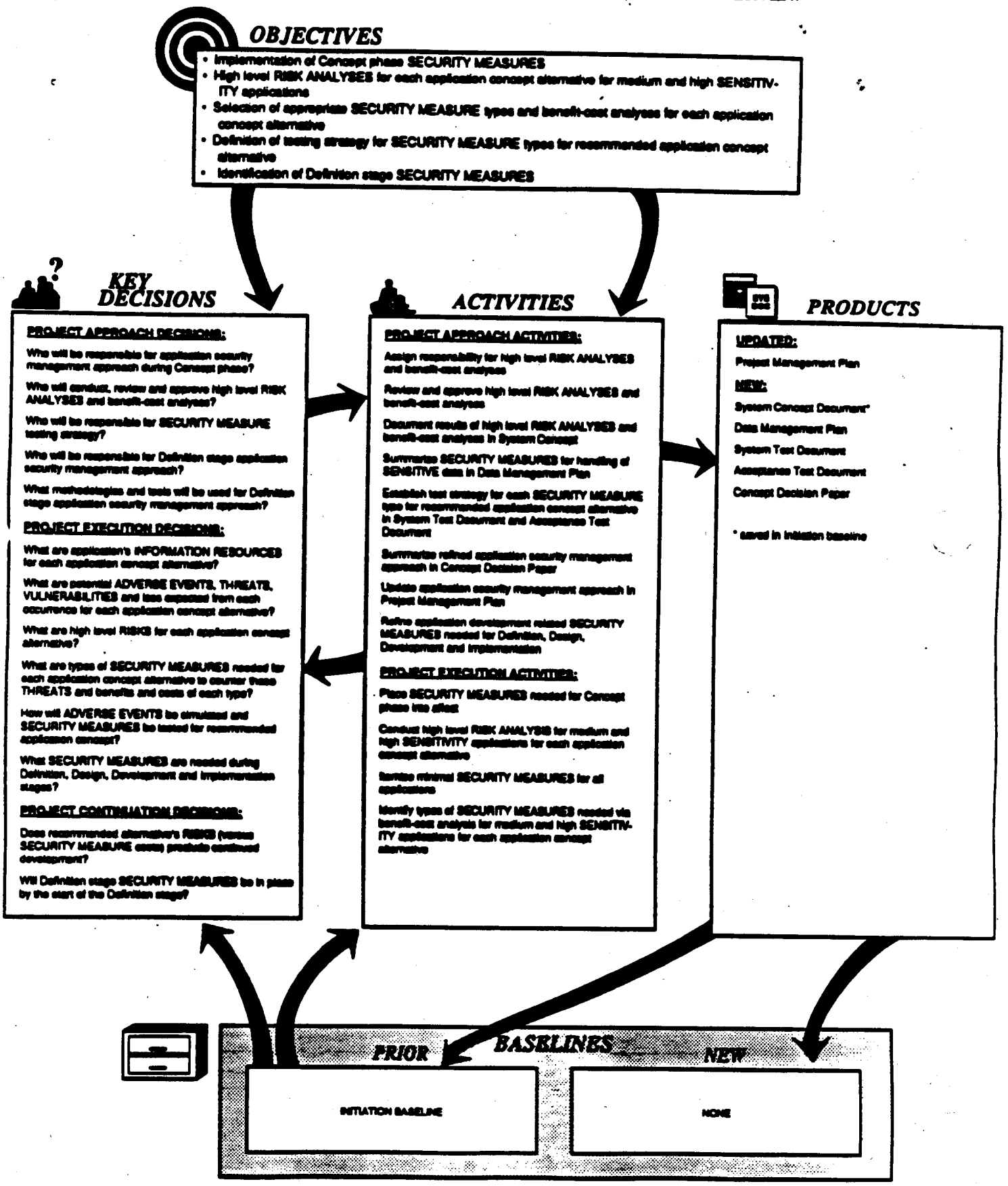
By the end of the *Concept phase* you will have:

- Identified the high level *RISKS* of each application concept alternative
- Identified the appropriate types of *SECURITY MEASURES* for each application concept alternative
- Conducted a more detailed *benefit-cost analysis* than in the *Initiation phase* for each application concept alternative
- Developed a testing strategy for each type of *SECURITY MEASURE* for the recommended application concept alternative
- Determined what *SECURITY MEASURES* need to be in place for the *Definition stage*

If you determined in the *Initiation phase* that your application has a low degree of *SENSITIVITY*, your task in the *Concept phase* is simple. This is because the "EPA Information Security Manual" spells out a set of minimal *SECURITY MEASURES*, which are all that are required for low *SENSITIVITY* applications. In addition, the cost of the agency's minimal *SECURITY MEASURES* are relatively negligible, so their cost need not be considered in the *benefit-cost analysis*.

Your methodologies for conducting *Concept phase activities* for medium and highly *SENSITIVE* applications relate to the degree of *SENSITIVITY*. In general, the more *SENSITIVE* the application, the greater the need for detailed, formal, quantitative methodologies; the less *SENSITIVE*, the more flexibility you have for summary level, informal, qualitative methodologies.

EXHIBIT 4.3-1: CONCEPT PHASE
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



4.3.2 . Concept Phase Activities

4.3.2.1 High Level Risk Analyses

For medium and highly *SENSITIVE* applications, your first *activity* is conducting a high level *RISK ANALYSIS* for each application concept alternative. While *RISK ANALYSIS* methodologies differ greatly, most include the identification of applicable *INFORMATION RESOURCES, ADVERSE EVENTS, THREATS, VULNERABILITIES,* and *RISKS.* Appendix C contains *ADVERSE EVENT, THREAT,* and *VULNERABILITY* Characterization Matrices which should help get your thinking started. "Guideline for Automatic Data Processing Risk Analysis" (FIPS PUB 65) contains more detailed information. The references in Appendix B offer other suggestions.

If the recommended application concept alternative includes the acquisition of an application specific installation (e.g., a PC) you should refer to Appendix C, Installation Risk Analysis, in the "EPA Information Security Manual," which provides you with several helpful worksheets and suggestions for documenting the results of your analysis. These worksheets will also be needed during the *Design stage.*

To illustrate a common *RISK ANALYSIS* methodology and how each of the core concepts relates, assume the following information management problem: you are in charge of implementing an efficient and effective way to process and document employee performance appraisal ratings. *INTEGRITY* and *CONFIDENTIALITY* would obviously be relevant to this problem. You might proceed as follows:

- Your first step is to identify the *INFORMATION RESOURCES* (e.g., employee performance data, computer platform, software)

- Second, you identify *ADVERSE EVENTS* that could affect the *INTEGRITY* and *CONFIDENTIALITY* of each *INFORMATION RESOURCE* (e.g., unauthorized manipulation of performance data or disclosure of performance data to other than the employee or authorized supervisor)

- Third, you identify *THREATS* that could cause these *ADVERSE EVENTS* (e.g., employees seeking to raise their scores, or employees seeking to find out the scores of others)

- Fourth, you identify the potential *VULNERABILITIES* (e.g., no user identification and authentication via hardware or software)

- Fifth, you identify the *RISK* for each *ADVERSE EVENT* (e.g., fairly low expectancy that a given employee would raise his/her own performance

appraisal score because of the known integrity of staff, medium likelihood of embarrassment over disclosure of confidential information)

Your *approach* needs to be forward-looking enough to anticipate future *RISKS*. For example, if there is a possibility that your database may, at some future time, include confidential business information (CBI), it might make sense to include access protection from the start. Keep in mind that good *SECURITY MEASURES* are often difficult and expensive to retrofit, so that over-designing in the short term may be a wise decision.

4.3.2.2 Selection of Security Measure Types and Benefit-Cost Analyses

Your next *activity* involves the selection, at a high level, of appropriate types of *SECURITY MEASURES* for each application concept alternative. The term "appropriate" implies both of the following:

- That the type of *SECURITY MEASURE* is effective
- That the *SECURITY MEASURE* type would cost less to implement over the *life cycle* than the *RISK* of not implementing it

Since selecting appropriate types of *SECURITY MEASURES* is a form of *benefit-cost analysis*, be sure to reference that practice paper. In this context, benefits are equated to the amount *RISK* is reduced as *VULNERABILITIES* are reduced or eliminated. Costs are equated to the cost for development, acquisition, implementation, operation, periodic evaluation and eventual archiving of the *SECURITY MEASURES*.

There are a number of things to keep in mind as you select types of *SECURITY MEASURES*:

- Some of the types of *SECURITY MEASURES* you require may already be planned for or in place. For example, the "EPA Information Security Manual" requires the implementation of minimal *SECURITY MEASURES* for all agency minicomputers, mainframe, PCs, LANs, and word processor installations. Of course, you still need to coordinate with the installation custodian to make sure that your requirements will be met.
- There are also a number of types of *SECURITY MEASURES* that are derived simply from following OSWER's Life Cycle Management Guidance. For example, quality assurance, *data management* and *configuration management* practices reduce your *VULNERABILITIES* to loss of *AVAILABILITY* and *INTEGRITY* and to *INAPPROPRIATE USE* at no additional cost. The cost of these *SECURITY MEASURE* types is accounted for under those *activities*.

Appendix C contains a Security Measure Characterization Matrix which should be helpful to you in identifying types of *SECURITY MEASURES.*

4.3.2.3 Test Strategy for Security Measures

During the *Concept phase,* you must also decide on a test strategy which will ensure that:

- All *SECURITY MEASURE* types for the recommended application concept alternative will be in place when they are needed
- They are functioning effectively
- They will remain effective over the entire *life cycle*

Your testing strategy should also reflect the relevance of the *SECURITY OBJECTIVES* (i.e., more rigorous testing for highly *SENSITIVE* applications; less rigorous testing for applications with medium *SENSITIVITY*). For example, if *CONFIDENTIALITY* were highly relevant, your strategy might be to exercise every line of code in the access control software; if *AVAILABILITY* were highly relevant, your test strategy might be to hold frequent disaster recovery drills.

Your strategy should include simulation of *ADVERSE EVENTS.* For example, a simulation of an *ADVERSE EVENT* relevant to *CONFIDENTIALITY* would be an attempt to subvert access *SECURITY MEASURES.*

4.3.3.3 Special Considerations for Developmental Security Measures During the Concept Phase

Your first concern, prior to conducting any of the above *activities,* is getting all your *Concept phase* developmental *SECURITY MEASURES* in place. For example, you may need to set up a process for personnel screening and selection or for controlled document handling prior to the start of any of the *Concept phase activities.*

4.3.4 · Concept Phase Products and Baselines

System Concept Document

You use the *System Concept* document to describe the:

- *SECURITY MEASURE* types for each application concept alternative, as part of the process of itemizing the *high level functional requirements* and *high level data requirements*

- *Life cycle* benefits and costs by *SECURITY MEASURE* type for each application concept alternative

Data Management Plan

You document your application security management *approach* for data *AVAILABILITY, INTEGRITY, CONFIDENTIALITY,* and *APPROPRIATE USE* in the *Data Management Plan.* You should be able to identify *SENSITIVE* data at the entity level at this *phase.* Refer to the practice paper on Data Management in Part 3 of the OSWER System Life Cycle Management Guidance.

Data specific *SECURITY MEASURES* (e.g., backup/recovery, logging and auditing) are also topics included in the *Data Management Plan* outline given in Part 2 of the OSWER System Life Cycle Management Guidance.

System Test Document and Acceptance Test Document

You document your test strategy for each type of *SECURITY MEASURE* for the recommended application concept in the *System Test Document* and the *Acceptance Test Document.* Since at this point you don't know how specific *SECURITY MEASURES* will be designed, this information will of necessity be quite general. You will, however, be able to define what *ADVERSE EVENTS* need to be simulated by the testing process.

Concept Decision Paper

At the end of the *Concept phase* you update the summary of your overall application security management *approach* in the *Concept Decision Paper.*

Project Management Plan

Also at the end of the *Concept phase,* you update your overall security management *approach* for the remainder of the *life cycle.* You also update the *Project Management Plan* to reflect the *objectives* accomplished as well as the *key decisions*

made, *activities* completed or underway, costs, *products* delivered, and *baselines* modified. Be sure to include:

- Revision of *Initiation phase* topics
- Methodology for high level *RISK ANALYSIS*
- Results of *benefit-cost analysis*
- For applications with low *SENSITIVITY*, an explanation that only minimal *SECURITY MEASURES* are required and therefore a *RISK ANALYSIS* and *benefit-cost analysis* were not conducted
- For applications with medium or high *SENSITIVITY*, reference the *System Concept* Document (above) for a description of *SECURITY MEASURE* types and costs

You also need to develop and document an application security management *approach* workplan for the *Definition stage*. It should cover new *objectives*, *key decisions*, *activities*, *products* and *baselines*. Be sure to address:

- *SECURITY MEASURES* needed to be in place at the start of the *Definition stage*
- The methodology to be used to define *SECURITY MEASURE* types
- The methodology to be used to define *SECURITY MEASURE* test criteria
- *Definition stage activities*, as defined in Section 4.4

Refer to the topical outline for the *Project Management Plan* given in Part 2 of the OSWER System Life Cycle Management Guidance for the *Concept phase*. Note that it includes a section specifically entitled "Security Approach."

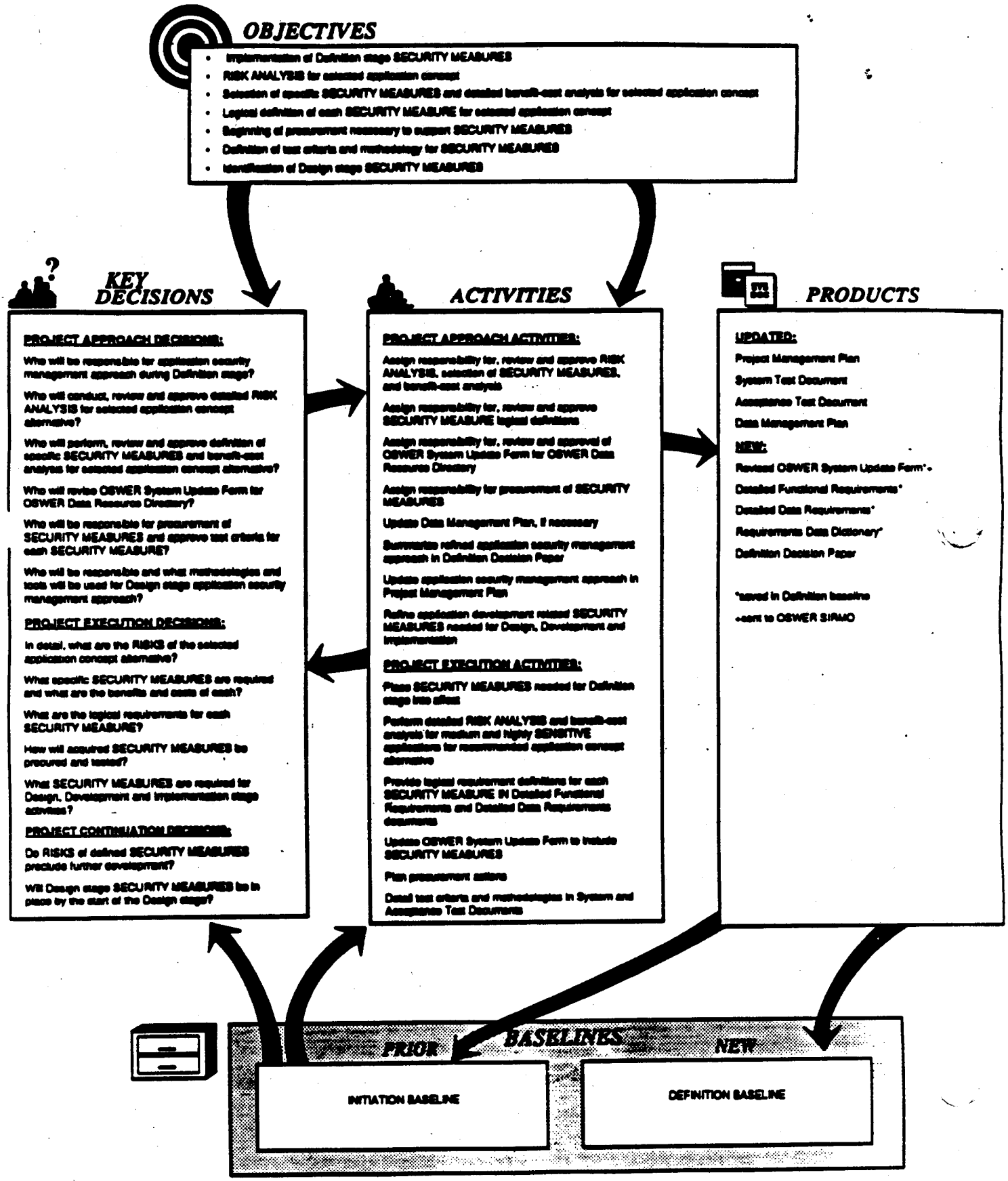
4.4 Application Security Management During the Definition Stage

4.4.1 Overview

You refined your application security management *approach* during the *Concept phase* after conducting *RISK ANALYSES* and *benefit-cost analyses* for each application concept alternative.

During the *Definition stage*, your *approach* addresses new project *objectives* and a number of new *key decisions*, *activities* and *products* along with the creation of the *Definition baseline*. See Exhibit 4.4-1 for an overview of these topics.

EXHIBIT 4.4-1: DEFINITION STAGE SUMMARY
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



By the end of the *Definition stage* you will have:

- Completed and documented a more rigorous *RISK ANALYSIS* of the selected application concept alternative
- Selected specific *SECURITY MEASURES* within each type identified in the *Concept phase* after performing a more detailed *benefit-cost analysis*
- Described each *SECURITY MEASURE* at a logical level of detail to allow for design of the software, logical database, external procedures, training courses, manuals, hardware, telecommunication equipment and facility construction
- Started preparation of purchase requests for physical and technical *SECURITY MEASURES* and the acquisition or modification of special installations and facilities
- Established your *SECURITY MEASURE* test criteria and defined your test methodology for the remainder of the *life cycle*
- Determined what *SECURITY MEASURES* need to be in place for the *Design stage*

4.4.2 Definition Stage Activities

4.4.2.1 Detailed Risk Analysis

If you have an application with high or medium *SENSITIVITY*, your first step is to conduct and document a *RISK ANALYSIS* of the selected application concept that is more detailed than the *RISK ANALYSES* you did for each of the alternatives during the *Concept phase*. Again, the level of formality depends on the degree of *SENSITIVITY* of your application. Refer to the citations in Appendix B of this document and the "EPA Information Security Manual" for more information on available methodologies.

4.4.2.2 Selection of Specific Security Measures and Detailed Benefit-Cost Analysis

You follow the *RISK ANALYSIS* with selection of specific *SECURITY MEASURES* from the types defined in the *Concept phase* and a much more detailed *benefit-cost analysis*. While methodologies for doing this vary, they all share the following elements:

- Selection of a broad range of specific *SECURITY MEASURES* which can effectively counter the potential *THREATS* and reduce the identified *VULNERABILITIES*

- Determination of costs to develop or acquire, install, operate, maintain, periodically evaluate and eventually archive these *SECURITY MEASURES*

- Comparison of the *life cycle* costs of comparably effective *SECURITY MEASURES*, choosing those which cost the least

- Selection of those *SECURITY MEASURES* with benefits which outweigh the costs (i.e., the most cost effective)

Chapter 9 of the "EPA Information Security Manual" describes a basic set of *SECURITY MEASURES* derived from "Guidelines for Security of Computer Applications" (FIPS PUB 73). Appendix C of this document also contains a Security Measures Characterization Matrix, broken down into logical categories, which should be helpful to you.

The selected SECURITY MEASURES should be added to the OSWER System Update Form.

4.4.2.3 Specific Security Measure Definition

You follow the selection of each specific *SECURITY MEASURE* with a detailed definition. Your definition descriptions must be at a level of detail to allow for the design of each individual physical, technical, administrative, or managerial *SECURITY MEASURE* in the next *stage*.

An example definition of a physical *SECURITY MEASURE* is:

> "REPORTS A, B, and C are to be shredded as soon as they are out-of-date."

An example definition for a technical *SECURITY MEASURE* might be:

> "No EMPLOYEE-RATE should exceed the MAX-RATE for the EMPLOYEE-POSITION. If this occurs, the Security Officer should be notified."

or:

> "Only the database administer is to have CREATE and DELETE access to the EMPLOYEE-POSITION-RATE-TABLE."

An example definition for an administrative *SECURITY MEASURE* is:

> "An employee must be denied access to the application immediately upon employee termination."

As shown in the above examples, *SECURITY MEASURE* definitions should be expressed in a way that give the designers freedom of implementation. The definitions can be expressed in English, as in the above examples, or in some tabular or other structured format, such as a Decision Tree.

4.4.2.4 Security Measure Procurement

If any of your selected *SECURITY MEASURES* need to be purchased, leased, built, contractor-supported, etc., now is the time to start planning your procurement actions.

4.4.2.5 Test Criteria for Security Measures

During the *Definition stage*, you define test criteria and methodologies for each specific *SECURITY MEASURE*.

Test criteria provide the basis for determining whether or not your *SECURITY MEASURES* are in place and functioning effectively. An example *SECURITY MEASURE* test criterion might be "no trivial passwords." You could measure password control software against this criterion as well as user practices during the *Implementation* and *Production stages*.

In your test methodology you define when each *SECURITY MEASURE* is to be tested, by whom, and how. You may chose to integrate testing of your technical software *SECURITY MEASURES* with all other software components during the *Design stage* through peer reviews, walkthroughs, modeling, etc. Other technical as well as physical and administrative *SECURITY MEASURES* may need to be tested or evaluated periodically throughout the application *life cycle* to ensure that they are in place and functioning effectively. For example, you may need to monitor user access privileges frequently or make sure that user passwords aren't taped to terminals.

4.4.3 Special Considerations for Developmental Security Measures During the Definition Stage

As during the *Concept phase,* your first concern is getting all your *Definition stage* developmental *SECURITY MEASURES* in place and reviewing the effectiveness of those already in place. For example:

- Do you need to control access to documentation?
- Have you identified who can authorize and who is authorized for each document?
- Do you have secure hardcopy storage available?
- How will confidential documents be identified and marked?

4.4.4 Definition Stage Products and Baselines

Be sure to keep in mind that the following *products* and *baselines* may contain definitions which you may need to keep confidential and that you may have to implement *SECURITY MEASURES* to protect them from inadvertent or intentional disclosure.

Revised OSWER System Update Form

You revise the OSWER System Update Form for the OSWER Data Resource Directory to include a description of the defined *SECURITY MEASURES* and submit this form to the OSWER Senior Information Resource Management Officer (SIRMO). The revised form is also placed in the *Definition baseline.*

Detailed Functional Requirements

You include the definition of each selected *SECURITY MEASURE* in the *Detailed Functional Requirements.*

Data Management Plan, Detailed Data Requirements, and Requirements Data Dictionary

You update your application security management *approach* for data *AVAILABILITY, INTEGRITY, CONFIDENTIALITY,* and *APPROPRIATE USE* in the *Data Management Plan.* Don't forget to include your *approach* for data conversion from hardcopy or existing databases if the data is *SENSITIVE.* The *Detailed Data Requirements* document has specific sections for "Audit Trail Requirements" and "Security Requirements." You describe access requirements (e.g., CREATE, READ,

UPDATE, DELETE) for each entity or data element for each user category in the *Requirements Data Dictionary*.

Refer to the Practice Paper on "Data Management" in Part 3 of the OSWER System Life Cycle Management Guidance.

System Test Document and Acceptance Test Document

You expand these two documents to include *SECURITY MEASURE* test criteria and methodologies as described above.

Definition Decision Paper

At the end of the *Definition stage* you update the summary of your overall application security management *approach* in the *Definition Decision Paper*.

Project Management Plan

At the end of the *Definition stage*, you update your overall application security management *approach* for the remainder of the *life cycle* in the *Project Management Plan*. You also update the *Project Management Plan* to reflect the *objectives* accomplished as well as the *key decisions* made, *activities* completed or underway, costs, *products* delivered, and *baselines* modified or added.

For applications with high or medium *SENSITIVITY*, be sure to include:

- Revision of *Concept phase* topics
- Results of detailed *RISK ANALYSIS*
- Reference to the *Detailed Functional Requirements* for definitions of each of the *SECURITY MEASURES*
- *Life cycle* costs of each *SECURITY MEASURE* in the *benefit-cost analysis* section
- Procurement approach for *SECURITY MEASURES* to be acquired
- Resources for *SECURITY MEASURE* procurement
- Handling of *SENSITIVE* data during conversion

You also need to develop and document an application security management *approach* workplan for the *Design stage*. It should cover new *objectives, key decisions, activities, products* and *baselines*. Be sure to address:

- *SECURITY MEASURES* needed to be in place at the start of the *Design stage*
- The methodology to be used to design each *SECURITY MEASURE*
- The methodology to be used to design the test procedure(s) for each *SECURITY MEASURE*
- *Design stage activities*, as defined in Section 4.5

Refer to the topical outline for the *Project Management Plan* given in Part 2 of the OSWER System Life Cycle Management Guidance for the *Definition stage*.

4.5 Application Security Management During the Design Stage

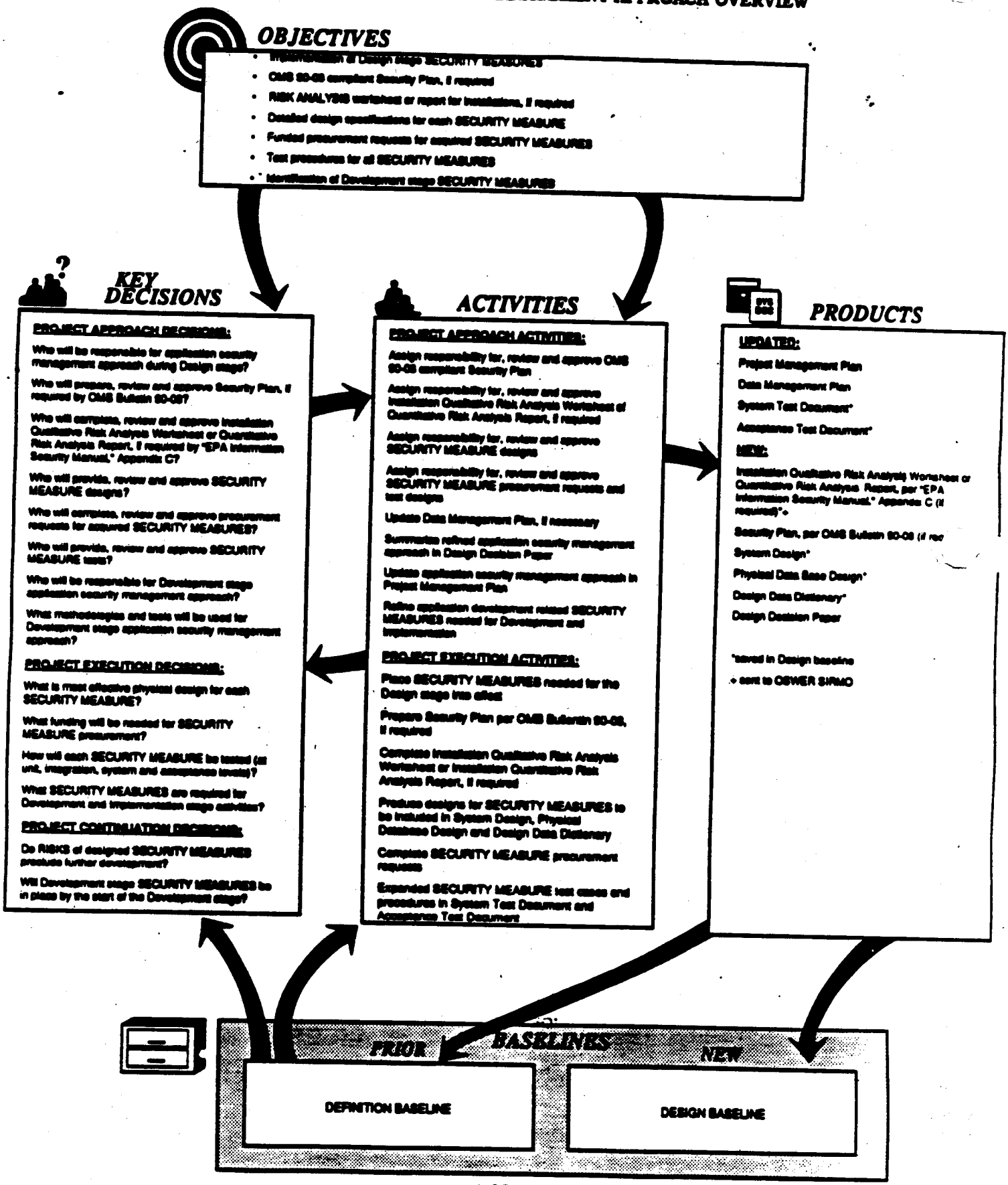
4.5.1 Overview

You planned your detailed application security management *approach* for the *Design stage* during the *Definition stage* by confirming the *Concept phase RISK ANALYSIS* and logically defining each needed *SECURITY MEASURE*. During Design your *approach* addresses new project *objectives* and a number of new *key decisions*, *activities* and *products*, as well as the creation of the *Design baseline*. See Exhibit 4.5-1 for an overview of these topics.

By the end of the *Design stage* you will have:

- Completed and submitted a Security Plan per OMB Bulletin 90-08, if required
- Confirmed the *RISK ANALYSIS* performed earlier and submitted appropriate worksheets and reports required for installations by the "EPA Information Security Manual"
- Specified each defined *SECURITY MEASURE* at a level of detail to allow for development of software, physical database, external procedures, training courses, user manuals, hardware, telecommunications equipment and facility construction
- Submitted funded procurement requests to the Procurement and Contracts Management Division and requisitions for acquisition or modification of special facilities to the appropriate organization
- Completed design of each defined *SECURITY MEASURE* test procedure
- Determined what *SECURITY MEASURES* need to be in place for the *Development stage*

EXHIBIT 4.5-1: DESIGN STAGE
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



4.5.2 Design Stage Activities

4.5.2.1 Special Oversight Organization Requirements

The Office of Management and Budget (OMB) requires the agency to submit plans for the "security and privacy" of "each computer system that contains sensitive information" to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for advice and comment. If you have an OSWER Level I application (as defined in Part 3, "System Life Cycle Review and Approvals") with medium or high *SENSITIVITY*, you will need to comply with OMB Bulletin 90-08. A citation is given in Appendix B. The Bulletin recommends a number of traditional *SECURITY MEASURES* for various types of applications which were compiled from other federal guidelines.

As noted in the *Initiation* and *Concept phases*, Appendix C of the "EPA Information Security Manual" describes methodologies for conducting application and installation *RISK ANALYSES*. Regardless of the *RISK ANALYSIS* methodology you chose to use during the *Concept phase* and *Definition stage*, for applications involving specific installations, you must complete a Qualitative Risk Analysis Worksheet or an Installation Quantitative Risk Analysis Report.

4.5.2.2 Security Measure Design Specifications

Your first step is preparing design specification for your physical, technical, administrative, and managerial *SECURITY MEASURES*. The following are examples of the level of detail appropriate for design specifications:

Physical: Paper Shredder

Heavy-duty
1/3 HP motor
Paper size up to 15' x 11'
Shreds = 1 1/2"
Up to 6 sheets of 20 lb paper
50' per minute

Technical: AUDIT REPORT #1A

If EMPLOYEE-RATE is greater than the MAX-RATE for the EMPLOYEE-POSITION:

then

post EMPLOYEE-NAME, EMPLOYEE-RATE, MAX-RATE for the EMPLOYEE-POSITION and VARIANCE-CODE of "13" in the SECURITY-NOTIFICATION-FILE

Technical: Design Data Dictionary (For each data entity or element)

Create Authority = GROUP A
Delete Authority = GROUP A
Update Authority = GROUP A and B
Read Authority = All

Administrative: Access Control Procedures

Prior to actual termination, an employee's immediate supervisor must provide the system administrator written notification of the termination date.

At COB of the termination date, all system access privileges will be revoked by the system administrator.

The *Design stage* is where you decide, along with your design team, how to actually implement each particular *SECURITY MEASURE*.

4.5.2.3 Security Measure Procurement

You also prepare design specifications for any hardware, software, telecommunications equipment, services and facility *SECURITY MEASURES* you are obtaining through procurement or requisition. Note that requests for special locks and combination safes go to the Facilities Management and Support Services Division. Don't forget that you may also need to incorporate *SECURITY MEASURES* in the procurement or requisition packages, themselves, such as contractor non-disclosure statements.

4.5.2.4 Security Measure Test Procedures

Based on the test criteria and methodologies you documented in the *Definition stage*, you design test procedures for each *SECURITY MEASURE* and add these procedures to the test documents. This includes tests for abnormal, unusual, improbable and illegal conditions and considers the effect of not following manual *SECURITY MEASURES*. In general your test procedures should include:

- descriptions of your test input (e.g., data and simulated *ADVERSE EVENTS*)

- expected results
- steps necessary to set up the test
- steps necessary to conduct the test

Keep in mind that some of your *SECURITY MEASURES* are tests themselves (e.g., a variance report), so at times you are testing the effectiveness of a test.

You may need to incorporate some formal testing techniques into the Test Documents for use in the *Development stage*. For example:

- Static evaluation includes:
  - code review
  - penetration studies
  - source code analyzers
- Dynamic testing includes:
  - execution of application with test data
  - program analyzers
  - flaw hypothesis method, based on analogous flaws in other applications

See "Guidelines for Security of Computer Applications" (FIPS PUB 73) for details.

4.5.3 Special Considerations for Developmental Security Measures During the Design Stage

As with the previous *phases* and *stage*, your first concern is getting all your *Design stage SECURITY MEASURES* in place and reviewing the effectiveness of those already in place. For example:

- Do you have technical access *SECURITY MEASURES* to prevent unauthorized use of your proprietary computer-based design tools?
- Do you need to have additional personnel screened and selected?
- Do you need to brief Procurement and Contracts Management Division on any *SENSITIVE* procurements?

Each member of the design team should be trained in the use of the design and programming tools and standards and be made particularly aware of the *VULNERABILITIES* of the *Design stage*. Typical techniques for avoiding these *VULNERABILITIES* include:

- Structured coding
- Avoiding unnecessary programming
- Isolation of user interfaces
- Human engineering, which makes interfaces easy to use and understand
- Avoidance of shared computer facilities, if possible
- Isolation of critical code
- Use of available *SECURITY MEASURES* provided by the Operating System

See "Guidelines for Security of Computer Applications" (FIPS PUB 73) for further suggestions.

Your effective management of the *Design stage* improves application security and reduces long-term costs: inadequate *SECURITY MEASURES* are difficult to improve without major redesign, and excessive costs for administrative *SECURITY MEASURES* may be needed later if the design exposes critical code or data. Also, the design review is the last opportunity to identify *VULNERABILITIES*.

4.5.4 Design Stage Products and Baselines

As in the *Definition stage*, you should keep in mind that these *products* and *baselines* may contain designs which may need to be kept confidential and that you may have to implement *SECURITY MEASURES* to protect them from inadvertent or intentional disclosure.

OMB Bulletin 90-08 Compliant Security Plan

If you have an OSWER Level I application (as defined in Part 3, "System Life Cycle Review and Approvals") with medium or high *SENSITIVITY*, OMB Bulletin 90-08 requires that a Security Plan for the recommended alternative be prepared and submitted by the agency to NIST/NSA. A format for this document is given in the Bulletin. The format highlights:

- Application identification and description

- The degree of *SENSITIVITY* assigned in the *Initiation phase*
- The *SECURITY MEASURES* identified for the selected application concept during the *Definition phase*
- Whether each *SECURITY MEASURE* is planned or already in place
- Additional comments such as the need for supplemental guidance or standards

When completed, submit the Security Plan to the OSWER Senior Information Resources Management Officer (SIRMO) for review and transmittal. This document also becomes part of the *Design baseline.* It is also updated, if necessary, during the *Implementation stage.*

Installation Risk Analysis Worksheet (Qualitative) or Report (Quantitative)

If your recommended application concept includes a dedicated installation you have already conducted your *RISK ANALYSIS* for the recommended alternative per Appendix C of the "EPA Information Security Manual" during the *Concept phase.* The worksheet or report should now be added to the *Design baseline.* A copy should also be sent to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in OSWER's annual security report to the Office of Information Resources Management (OIRM).

System Design document

You include the detailed physical designs of each defined *SECURITY MEASURE* in the *System Design* document.

Data Management Plan, Physical Database Design and Design Data Dictionary

You update your application security management *approach* for data *AVAILABILITY, INTEGRITY, CONFIDENTIALITY* and *APPROPRIATE USE* in the *Data Management Plan.* Refer to the Practice Paper on "Data Management" in Part 3 of the Guidance.

You specify access *SECURITY MEASURES* (if any) for each entity or element in the *Physical Database Design* and *Design Data Dictionary.*

System Test Document and Acceptance Test Document

You expand these two documents to include *SECURITY MEASURE* test procedures. Note that the design documents above provide the basis for a *SECURITY MEASURE* design validation and development of detailed *SECURITY MEASURE* testing procedures.

Design Decision Paper

At the end of the *Design stage* you update the summary of your overall application security management *approach* in the *Design Decision Paper.*

Project Management Plan

At the end of the *Design stage,* you update your overall application security management *approach* for the remainder of the *life cycle* in the *Project Management Plan.* You also update the *Project Management Plan* to reflect the *objectives* accomplished as well as the *key decisions* made, *activities* completed or underway, costs, *products* delivered, and *baselines* modified or added.

For applications with high or medium *SENSITIVITY,* be sure to include:

- Revision of *Definition stage* topics
- Planning issues for installation of *SECURITY MEASURES* and application security awareness and training

You also need to develop and document an application management *approach* workplan for the *Development stage.* It should cover new *objectives, key decisions, activities, products* and *baselines.* Be sure to address:

- *SECURITY MEASURES* needed to be in place at the start of the *Development stage*
- The methodology to be used to develop each designed *SECURITY MEASURE*
- The methodology to be used to perform unit and integration testing of each *SECURITY MEASURE*
- *Development stage activities,* as defined in Section 4.6

Refer to the topical outline for the *Project Management Plan* given in Part 2 of the OSWER System Life Cycle Management Guidance for the *Design stage*

4.6 Application Security Management During the Development Stage

4.6.1 Overview

You planned your detailed application security management *approach* for the *Development stage* during the *Design stage.* During development your *approach*

addresses new project *objectives* and a number of new *key decisions, activities,* and *products* along with the creation of the *Development baseline.* See Exhibit 4.6-1 for an overview of these topics.

By the end of the *Development stage* you will have:

- Developed (i.e., coded) each software *SECURITY MEASURE*
- Otherwise acquired or constructed each *SECURITY MEASURE*
- Performed unit and integration tests of each of the *SECURITY MEASURES*
- Drafted application security management aspects of operational documents
- Complied with "EPA Information Security Manual", Appendix D, guidance in preparation of an installation Continuity of Operations or application Contingency Plan as one of your *SECURITY MEASURES*
- Determined what *SECURITY MEASURES* need to be in place for the *Implementation stage*

4.6.2 Development Stage Activities

4.6.2.1 Coding of Security Measures

Your first step is coding your software *SECURITY MEASURES* such as user identification and authentication routines, audit trails, exception reporting, variance detection, anomalies in volumes, etc.

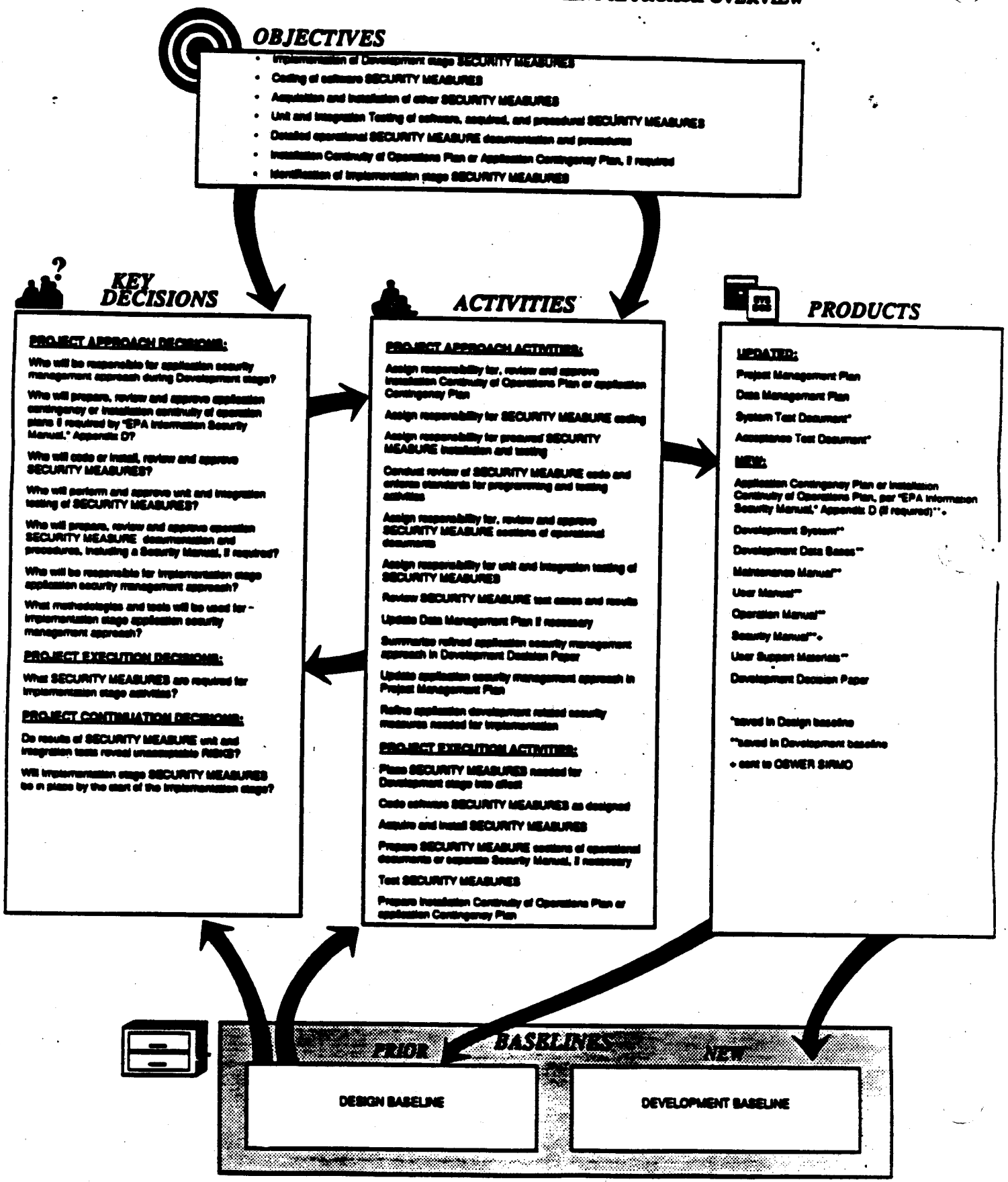
4.6.2.2 Acquisition of Procured Security Measures

Throughout the *Development stage* you accept and put into place the *SECURITY MEASURES* you procured or had built or modified.

4.6.2.3 Preparation of Operational Documents

You also write the *SECURITY MEASURE* sections of the *User, Maintenance* and *Operations Manuals,* draft a separate *Security Manual,* if appropriate, and prepare all application security awareness and training courses/modules and material.

EXHIBIT 4.6-1: DEVELOPMENT STAGE
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



The "EPA Information Security Manual," Appendix D, also requires an installation Continuity of Operations plan or application Contingency Plan for all high or medium *SENSITIVITY* applications where *AVAILABILITY* is a relevant *SECURITY OBJECTIVE*.

One common problem with Continuity of Operations Plans is the omission of procedures to restore operations at the original site. Don't neglect this important part of the process.

4.6.2.4 Unit and Integration Testing of Security Measures

At the same time you prepare test data for unit and integration testing and conduct these *SECURITY MEASURE* tests. This testing covers acquired (e.g., facilities, hardware, telecommunications devices) as well as coded (i.e. software) and procedural *SECURITY MEASURES*. It also includes testing of any procedural *SECURITY MEASURES* described in the operational documents.

4.6.3 Special Considerations for Developmental Security Measures During the Development Stage

As with the previous *phases* and *stages*, your first concern is getting all your *Development stage SECURITY MEASURES* in place and reviewing the effectiveness of those already in place. For example:

- Have your programmers been briefed on *SECURITY MEASURES*?
- How will you prevent or detect fraudulent changes to code?
- Are all developmental computers virus free?
- Do you have adequate procedures for disposing of *SENSITIVE* source and object code listings?
- Does the installation have a Continuity of Operations Plan for loss of your developmental computer or you for your key programmers?

Modern information engineering methods enhance application security, since they reduce both flaws in the implementation of *SECURITY MEASURES* and fraudulent additions or changes to code. Techniques include:

- Peer review
- Making one other programmer equally responsible

- Program library that:
  - permits only authorized persons to access modules
  - records all accesses
  - associates control data (e.g., record, byte counts) with modules
  - enables comparison of current version to previous versions
- Special documentation of *SECURITY MEASURE* related code
- Avoiding programmer association with operational application
- Redundant computation
- Program development tools such as:
  - high level languages
  - preprocessors
  - reformat source code
  - cross reference listings
  - debugging aids
  - 4GLs

"Guidelines for Security of Computer Applications" (FIPS PUB 73) provides further details.

4.6.4 Development Stage Products and Baselines

Keep in mind that you may need to handle these documents as *SENSITIVE* information, as in the *Definition* and *Design stages.*

Installation Continuity of Operations Plan or Application Contingency Plan

The *Development baseline* also includes the installation Continuity of Operations Plan or application Contingency Plan, if required by the "EPA Information Security Manual," Appendix D. A copy should be sent to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in the OSWER annual security report to the Office of Information Resources Management (OIRM).

The plan should cover:

- Maximum acceptable period of interruption
- Identification of critical functions
- Alternate processing installations and facilities
- Backup and recovery procedures and drills

Details are available in "Guidelines for Security of Computer Applications" (FIPS PUB 73) and the "EPA Information Security Manual," Appendix D.

Security Manual

If necessary, write a separate *Security Manual*. An outline is provided in Part 2 of the OSWER System Life Cycle Management Guidance. This is also submitted to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in the annual security report for the Office of Information Resources Management (OIRM).

Maintenance Manual, Operations Manual, User Manual and User Support Materials

Review the outlines of each of these operational documents (Part 2 of the OSWER System Life Cycle Management Guidance) and provide input concerning *SECURITY MEASURE* aspects, if not already covered by a separate *Security Manual*.

Source Code Comments

The OSWER System Life Cycle Management Guidance recommends that source code comments be used in general to document the details of any module. However, you should be aware that there is a tradeoff between good documentation practices and introducing a potential *VULNERABILITY* by using detailed comments in *SECURITY MEASURE* related code, because these comments could be used by hackers to determine how to circumvent the *SECURITY MEASURES*.

System Test Document and Acceptance Test Document

You update your *SECURITY MEASURES* test procedures and document your unit and integration test results in the *System Test Document* and the *Acceptance Test Document*. Where applicable, you include both test data and results since these will be used periodically throughout the *life cycle* for regression testing. Test results should be reviewed for previously uncovered *VULNERABILITIES*.

Development Decision Paper

At the end of the *Development stage*, you update the summary of your overall application security management *approach* in the *Development Decision Paper*, and summarize the results of the *Development stage*, particularly testing, regarding application security. Document any new *VULNERABILITIES* that have been revealed by the testing process.

Project Management Plan

At the end of the *Development stage*, you update your overall application security management *approach* for the remainder of the *life cycle* in the *Project Management Plan*. You also update the *Project Management Plan* to reflect the *objectives* accomplished as well as the *key decisions* made, *activities* completed or underway, costs, *products* delivered, and *baselines* modified or added.

For applications with high or medium *SENSITIVITY*, be sure to include:

- Revision of *Design stage* topics
- Planning issues for installation of *SECURITY MEASURES* and application security awareness and training

You also need to develop and document an application security management *approach* workplan for the *Implementation stage*. It should cover new *objectives*, *key decisions*, *activities*, *products* and *baselines*. Be sure to address:

- *SECURITY MEASURES* needed to be in place at the start of the *Implementation stage*
- The methodology to be used to complete implementation of each *SECURITY MEASURE*
- The methodology to be used to perform system and acceptance testing for each *SECURITY MEASURE*
- *Implementation stage activities*, as defined in Section 4.7

Refer to the topical outline for the *Project Management Plan* given in Part 2 of the OSWER System Life Cycle Management Guidance for the *Development stage*.

Data Management Plan

Revise the *Data Management Plan*, if necessary. Refer to the Practice Paper on "Data Management" in Part 3 of the Guidance.

4.7 Application Security Management During the Implementation Stage

4.7.1 Overview

You planned your detailed application security management *approach* for the *Implementation stage* during the *Development stage*. During implementation your *approach* addresses new project *objectives*, and a number of new *key decisions, activities*, and *products* as well as the updated *Development baseline*. See Exhibit 4.7-1 for an overview of these topics.

By the end of the *Implementation stage* you will have:

- Performed system and acceptance testing of all *Production stage SECURITY MEASURES*
- Trained everyone who has a application security role and reported the results of this training
- Completed the Application Certification Worksheet
- Updated the OMB Bulletin 90-08 compliant Security Plan drafted in the *Design stage*
- Determined what *SECURITY MEASURES* need to be in place for the *Production stage*

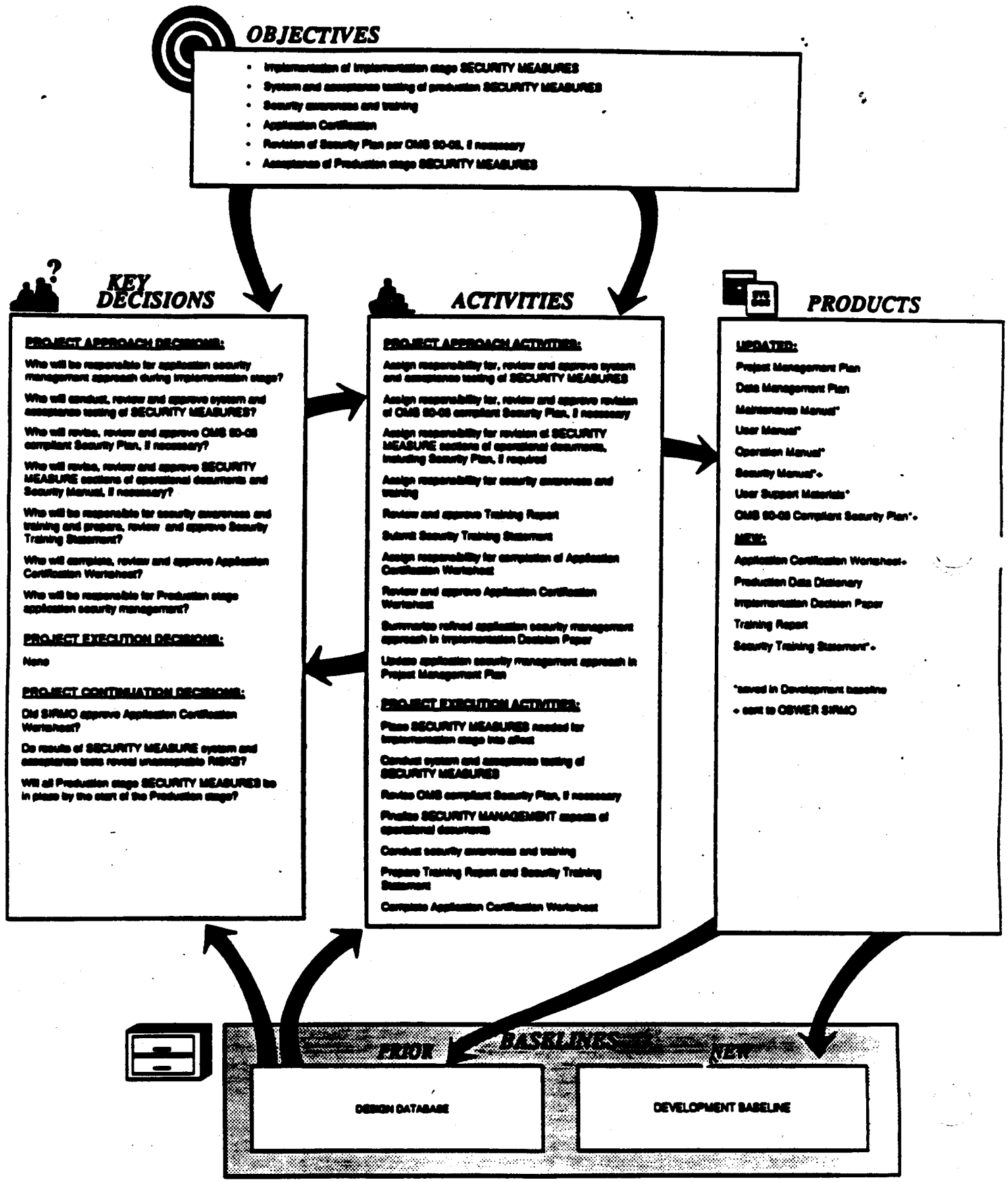
4.7.2 Implementation Stage Activities

4.7.2.1 System and Acceptance Testing of Security Measures

You develop test inputs (e.g., data and simulated *ADVERSE EVENTS*) and conduct penetration, system and acceptance testing on each *SECURITY MEASURE* to be placed into *production*. You may choose to test your software *SECURITY MEASURES* along with the testing of other software components or to test them separately.

During system testing you ensure that all *SECURITY MEASURES* are compatible with each other as well as other application requirements. For example, software *SECURITY MEASURES* should not seriously degrade system response times. Identification and authentication protocols should not significantly impede need-to-know access.

EXHIBIT 4.7-1: IMPLEMENTATION STAGE
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



During acceptance testing, you make sure that your *SECURITY MEASURES* adequately support each of the relevant OSWER *SECURITY OBJECTIVES.*

4.7.2.2 Application Security Awareness and Training

The "EPA Information Security Manual" requires that training itself be a *SECURITY MEASURE.* You conduct general application security awareness and specific task training during the *Implementation stage,* either in conjunction with other user training or separately, so that all personnel with an application security role will be in a position to fulfill their roles when the system goes into *production.* Be sure to think broadly when identifying people for training: you may need to include such diverse staff as managers, data generators, information disseminators, facility operators, software and hardware maintainers, etc. Prepare a statement that security awareness and training have been conducted for all appropriate personnel.

4.7.2.3 Completion of Application Certification Worksheet

If the application is of medium or high *SENSITIVITY,* you complete the Application Certification Worksheet found in Appendix B of the "EPA Information Security Manual." Note that the manual states that the worksheet be completed by the application owner, reviewed by the owner's immediate supervisor, and approved by the OSWER Senior Information Resource Management Officer (SIRMO).

4.7.2.4 Revision of OMB Bulletin 90-08 Compliant Security Plan

If necessary, you revise the OMB Bulletin 90-08 compliant Security Plan drafted during the *Design stage.*

4.7.3 Special Considerations for Developmental Security Measures During the Implementation Stage

As with the previous *phases* and *stages,* your first concern is getting all your *Implementation stage SECURITY MEASURES* in place and reviewing the effectiveness of those already in place. For example:

- If you are converting an existing manual or automated database are you adequately protecting the *SENSITIVE* data during transfer?
- Have your trainers been screened?

- Is there a procedure for reporting *ADVERSE EVENTS* during system and acceptance testing?

- Are you protecting your copyrighted software?

4.7.4 Implementation Stage Products and Baselines

Updated OMB Bulletin 90-08 Compliant Security Plan

If necessary, an updated version of the Security Plan required by OMB Bulletin 90-08 is submitted to the OSWER Senior Information Resources Management Officer (SIRMO).

Security Training Statement

Submit your Security Training Statement to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in the annual security report for the Office of Information Resources Management (OIRM). The *Implementation baseline* includes a copy of the Security Training Statement.

Application Certification Worksheet

The *Implementation baseline* includes the completed and approved Application Certification Worksheet. It is also submitted to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in the annual security report to the Office of Information Resources Management (OIRM).

Security Manual

The *Implementation baseline* also includes the *Security Manual*, revised if necessary based on the results of *SECURITY MEASURE* testing (i.e. failure of any documented procedural *SECURITY MEASURE*). It is also sent to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in the annual security report to the Office of Information Resources Management (OIRM).

Maintenance Manual, Operations Manual, Users Manual, and User Support Materials

This is the last chance to revise the *SECURITY MEASURE* sections of any operational documents before the *Production stage.*

Training Report

You document the results of the application security awareness and training (along with any other training) in the *Training Report*, in addition to the Security Training Statement mentioned above.

System Test Document and Acceptance Test Document

You document the results of system and acceptance testing of each *SECURITY MEASURE* in the *System Test Document* and the *Acceptance Test Document*.

Implementation Decision Paper

At the end of the *Implementation stage*, you update the summary of your overall application security management *approach* in the *Implementation Decision Paper*. The decision to take the application into *production* should stress the results of *SECURITY MEASURE* system and acceptance testing.

Project Management Plan

At the end of the *Implementation stage*, you update your overall application security management *approach* for the remainder of the *life cycle* in the *Project Management Plan*. You also update the *Project Management Plan* to reflect the *objectives* accomplished as well as the *key decisions* made, *activities* completed or underway, costs, *products* delivered, and *baselines* modified or added.

For applications with high or medium *SENSITIVITY*, be sure to include:

- Revision of *Development stage* topics
- Results of SECURITY MEASURE installation and testing and application security awareness and training

You also need to develop and document an application management *approach* workplan for the *Production stage*. It should cover new *objectives*, *key decisions*, *activities*, *products* and *baselines*. Be sure to address:

- *SECURITY MEASURES* needed to be in place at the start of the *Production stage*
- *Production stage activities*, as defined in Section 4.8

Refer to the topical outline for the *Project Management Plan* given in Part 2 of the OSWER System Life Cycle Management Guidance for the *Implementation stage*.

Data Management Plan

Revise the *Data Management Plan,* if necessary. Refer to the Practice Paper on "Data Management" in Part 3 of the Guidance.

4.8 Application Security Management During the Production Stage

4.8.1 Overview

You completed your detailed application security management *approach* for the *Production stage* during the *Implementation stage,* by completely testing and certifying all *SECURITY MEASURES.* During the *Production stage* your *approach* may alter operational project *objectives,* and affect a number of *key decisions, activities,* and *products* and contribute to the *Operational baseline.* See Exhibit 4.8-1 for an overview of these topics.

Application security management during the *Production stage* involves:

- Operation and monitoring of *SECURITY MEASURES*
- Responding to *ADVERSE EVENTS*
- Submitting modification requests
- Ongoing application security awareness and training

4.8.2 Production Stage Activities

4.8.2.1 Operation and Monitoring of Security Measures

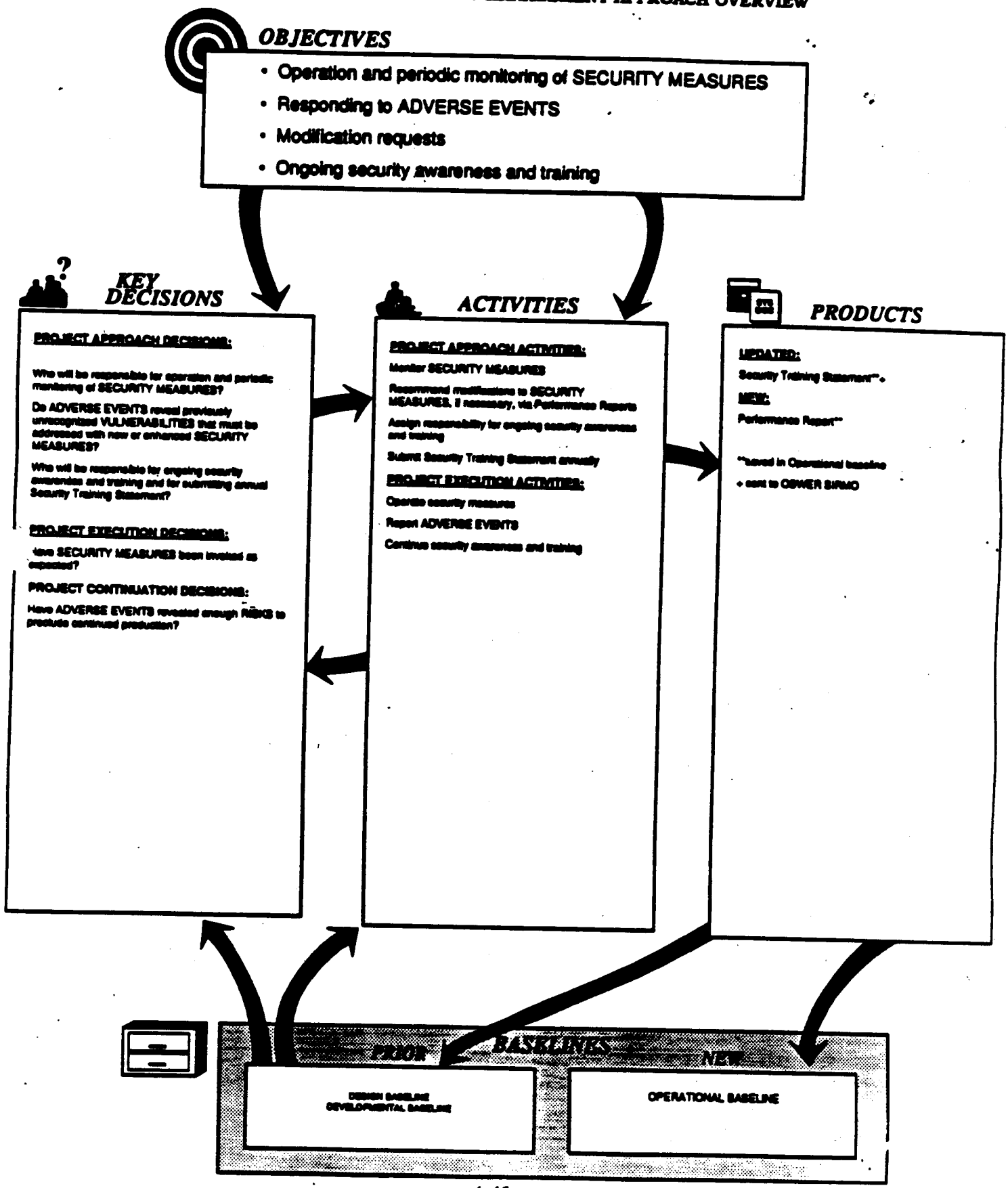
SECURITY MEASURES are now operating. Periodically, you may supplement these routine *SECURITY MEASURES* by conducting informal inspections, such as spot review of log sheets.

4.8.2.2 Responding to Adverse Events

During the *Production stage,* you must deal with *ADVERSE EVENTS* as they occur. Your administrative *SECURITY MEASURES* should have detailed procedures for handling these situations. For example, what steps would you take if an employee intentionally introduced a virus into the application, mishandled confidential business information, or shared a password?

In addition, application Contingency Plans or installation Continuity of Operations Plans may be invoked by *ADVERSE EVENTS.* For example, a Contingency Plan may be executed in response to the loss of a database. In response to a fire or flood or hardware failure you will invoke a Continuity of Operations plan.

EXHIBIT 4.8-1: OPERATION STAGE
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



4.8.2.3 Modification Requests

You may uncover new *VULNERABILITIES* during the *Production stage* as the result of day-to-day operation of *SECURITY MEASURES*. These should be handled according to established OSWER System Life Cycle Management Guidance *Configuration Management* procedures in Part 3.

4.8.2.4 Ongoing Application Security Awareness and Training

You need to repeat application security awareness and training as performed in the *Implementation stage* for new employees, transferred employees, and periodically as a refresher for existing employees. Update your Security Training Statement as appropriate.

4.8.3 Production Stage Products and Baselines

Security Training Statement

Submit your Security Training Statement to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in the annual security report for the Office of Information Resources Management (OIRM). The *Implementation baseline* includes a copy of the Security Training Statement.

Performance Report

You may wish to summarize *ADVERSE EVENTS* and failures of *SECURITY MEASURES* using the *Performance Report* format provided by Part 2 of the OSWER System Life Cycle Management Guidance.

Other Life Cycle Documents

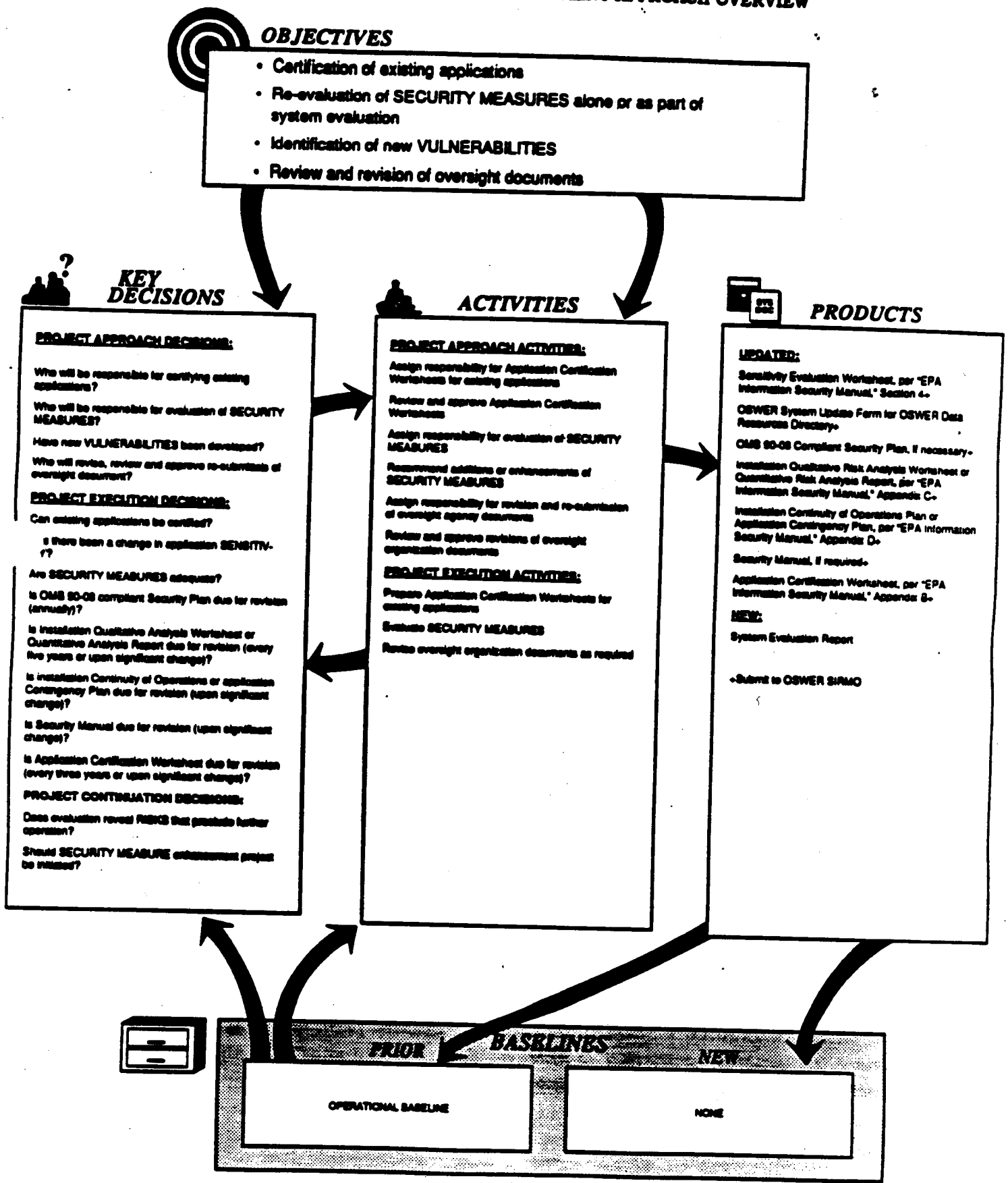
You may revise the *SECURITY MEASURE* sections of other documents as necessary via OSWER System Life Cycle Management Guidance *Configuration Management* procedures (Part 3).

4.9 Application Security Management During the Evaluation Stage

4.9.1 Overview

Periodic formal evaluation under the OSWER System Life Cycle Management Guidance monitors the operational project *objectives*, and addresses a number of new *key decisions, activities*, and *products* and possibly alters the *Operational baseline*. See Exhibit 4.9-1 for an overview of these topics.

EXHIBIT 4.9-1: EVALUATION STAGE
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



Application security management during the *Evaluation stage* involves:

- Certifying existing applications
- Uncovering new *VULNERABILITIES* and recommending enhancements or additions to *SECURITY MEASURES* as part of an overall system evaluation as part of the *life cycle*
- Analyzing occurrences of *ADVERSE EVENTS* that represents a significant change in application security requirements and therefore re-evaluation.
- Conducting appropriate evaluation and resubmitting oversight organization documents as required

4.9.2 Evaluation Stage Activities

4.9.2.1 Certification of Existing Applications

All existing applications that have not yet been certified during the *Implementation stage* must undergo a formal evaluation process and be certified for application security using the process suggested in the "EPA Information Security Manual," Appendix B, including *SENSITIVITY* evaluation and *RISK ANALYSIS*. Poorly designed applications may have to be upgraded through the *life cycle* process before certification is possible.

Using the *VULNERABILITIES* uncovered in this *RISK ANALYSIS*, you can reduce obvious *RISKS* immediately while taking the time to plan more thorough *SECURITY MEASURES* and revise the application system using the *life cycle approach*. This allows for integrating application security improvements with other purposes.

4.9.2.2 Security Enhancements

Enhancements to application security are handled through the *life cycle* as described above, with one exception: proposed enhancements must be scrutinized for impact on application security along with an evaluation of the *INTEGRITY* and motivation of the person making the request.

4.9.2.3 Resubmission of Oversight Documents

Various oversight documents need to be resubmitted on a periodic basis (refer to Exhibit 4.1-1), as follows:

- The OMB Bulletin 90-08 Compliant Security Plan must be resubmitted annually
- The Installation Qualitative Risk Analysis Worksheet or Quantitative Risk Analysis Report must be resubmitted every five years
- The Application Certification Worksheet must be resubmitted every three years

The following documents must be updated when significant changes occur or as needed (refer to Exhibit 4.1-1):

- Table for Sensitivity Evaluation
- OSWER System Update Form
- The Installation Qualitative Risk Analysis Worksheet or Quantitative Risk Analysis Report, if applicable
- Installation Continuity of Operations Plan or application Contingency Plan, if applicable
- Security Manual, if applicable
- Application Certification Worksheet

4.9.3 Evaluation Stage Products and Baselines

Table for Sensitivity Evaluation

Use this worksheet from the "EPA Information Security Manual," Section 4, to help certify existing applications and also to evaluate enhancements. Submit it to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in the annual security report to the Office of Information Resources Management (OIRM).

OSWER System Update Form

Revise this form when significant changes occur. Submit it to the OSWER Senior Information Resource Management Officer (SIRMO) for the OSWER Data Resource Directory.

OMB Bulletin 90-08 Compliant Security Plan

Resubmit the Security Plan to the OSWER Senior Information Resource Management Officer (SIRMO) every year for inclusion in the annual security report to the Office of Information Resources Management (OIRM).

Installation Risk Analysis Worksheet or Report

Resubmit the appropriate Risk Analysis Worksheet or Report, if required by the "EPA Information Security Manual," Appendix C, to the OSWER Senior Information Resource Management Officer (SIRMO) every five years and when significant changes occur for inclusion in the annual security report to the Office of Information Resources Management (OIRM).

Installation Continuity of Operations Plan or Application Contingency Plan

Resubmit the appropriate installation Continuity of Operations Plan or application Contingency Plan, if required by the "EPA Information Security Manual," Appendix D, to the OSWER Senior Information Resource Management Officer (SIRMO) when significant changes occur for inclusion in the annual security report to the Office of Information Resources Management (OIRM).

Security Manual

Revise the Security Manual, if required, and submit it to the OSWER Senior Information Resource Management Officer (SIRMO) for inclusion in the annual security report to the Office of Information Resources Management (OIRM).

Application Certification Worksheet

Submit the Application Certification Worksheet to the OSWER Senior Information Resource Management Officer (SIRMO) for certifying existing applications and for re-certifying every three years and when significant changes occur.

System Evaluation Report

Use the *System Evaluation Report* as a mechanism for periodic evaluation of the application security aspect of the project. Its outline includes a section specifically for security and a general section for functional and data improvements. Refer to Part 2 of this guidance.

4.10 Application Security Management During the Archive Stage

4.10.1 Overview

SENSITIVE information and applications may remain *SENSITIVE* for a period of time even after the application has been archived. During the *Archive stage* you identify archive project *objectives*, and address a number of new *key decisions, activities*, and *products* along with the archiving of the *Operational baseline*. See Exhibit 4.10-1 for an overview of these topics.

Application security management during the *Archive stage* involves:

- Seeing that *SECURITY MEASURES* for disposition of all *INFORMATION RESOURCES* are carried out correctly
- Certifying the disposition of archived documents and magnetic media to see that each is destroyed and/or stored appropriately

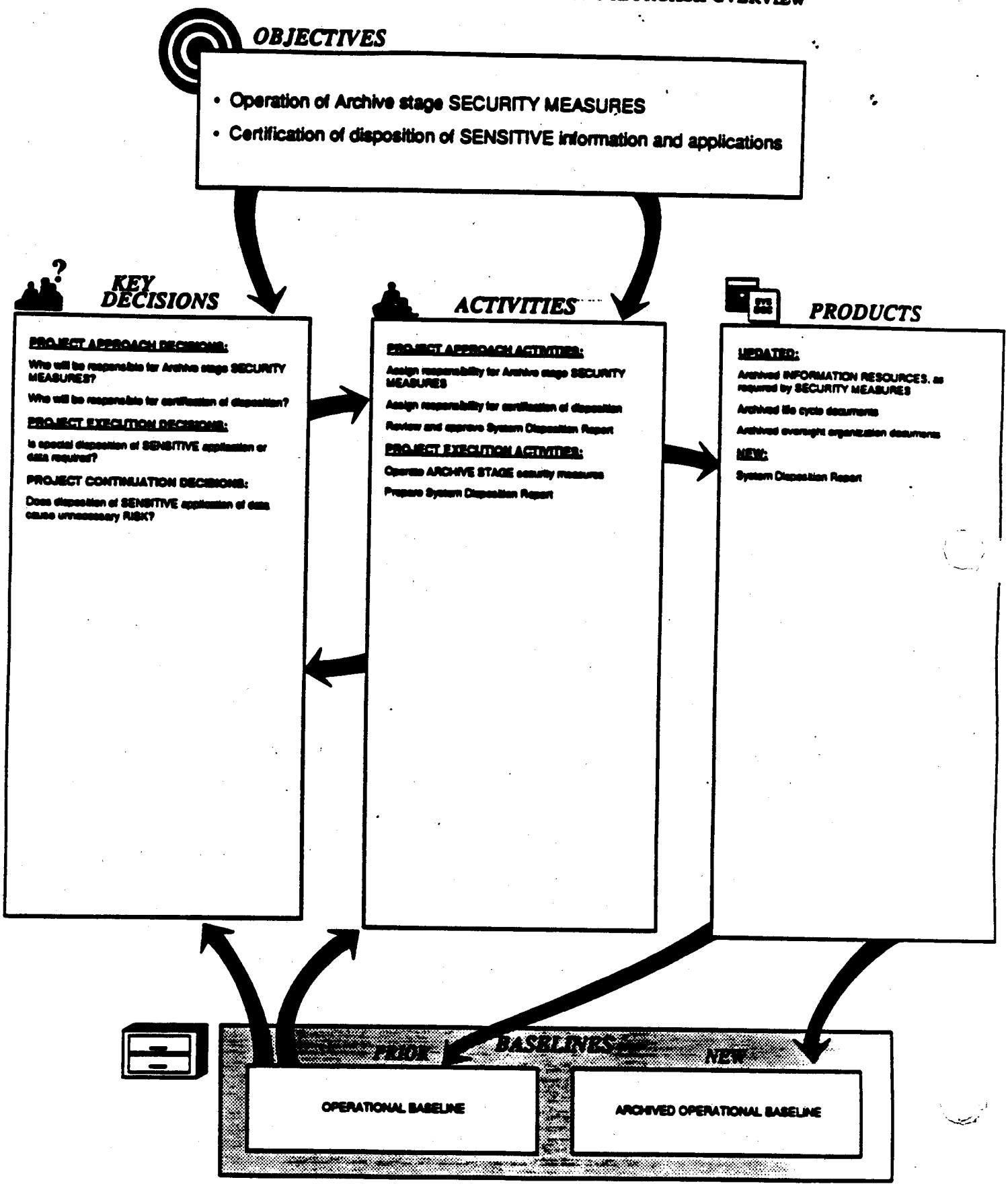
4.10.2 Archive Stage Activities

4.10.2.1 Disposition of Security Measures

You should revisit the Sensitivity Evaluation worksheet from the *Initiation phase* and *RISK ANALYSIS* from the *Concept phase* to help determine the potential *RISKS* involved in archiving. The retention period for *SENSITIVE* information should be considered.

Here you will carry out any *SECURITY MEASURES* designed during the *life cycle* for the *Archive phase* (e.g., degaussing tapes, re-initializing memory, shredding documents or securely storing documents, revoking accounts and passwords, debriefing personnel).

EXHIBIT 4.10-1: ARCHIVE STAGE
APPLICATION SECURITY MANAGEMENT APPROACH OVERVIEW



4.10.2.2 Certification of Archive Process

The *System Disposition Report* is the vehicle for certifying the disposition of *INFORMATION RESOURCES*, including *life cycle* and oversight organization documents.

4.10.3 Archive Stage Products and Baselines

System Disposition Report

You use the *System Disposition Report* to ensure and document that appropriate *SECURITY MEASURES* are used during the *archival* process. You must secure the archived *Operational baseline* appropriately. Keep in mind that stored material may have to be reinstated at a later time along with applicable *SECURITY MEASURES*.

Appendix A: Terms

This appendix provides a glossary of terms that are either OSWER core concepts (defined further, with examples, in Chapter 2) or definitions derived from other sources. Multiple definitions and synonyms are provided to resolve potential discrepancies between this document and other applicable guidance documents.

Adverse Event

OSWER Core Concept:

In the broadest sense, the loss of an application's *AVAILABILITY, INTEGRITY, CONFIDENTIALITY* or *INAPPROPRIATE USE* are *ADVERSE EVENTS.* Anything that adversely affects any application *INFORMATION RESOURCE* is also an *ADVERSE EVENT* since this in turn results in loss of *AVAILABILITY, INTEGRITY, CONFIDENTIALITY* or *INAPPROPRIATE USE* or takes additional resources to replace or recover.

Application Security

Other definition:

The set of controls that makes an information system perform in an accurate and reliable manner, only those functions it was designed to perform. The set of controls includes the following: programming, access, source document, input data, processing storage, output and audit trail. (EPA Information Security Manual, Appendix A, "Information Security. ")

Appropriate Use/Inappropriate Use

OSWER Core Concept:

While *INAPPROPRIATE* use or misuse of an application may not result in direct loss of *AVAILABILITY, INTEGRITY,* or *CONFIDENTIALITY,* misuse of our *INFORMATION RESOURCES* is clearly undesirable and sometimes unlawful. In OSWER we want to ensure that our applications are used for, and only for, support of our programmatic mission.

Availability

OSWER Core Concept:

OSWER develops applications to support our programmatic mission. The loss of *AVAILABILITY* of any *INFORMATION RESOURCE* associated with an application could affect the application's ability to support some aspect of the mission. *AVAILABILITY* refers to our need to have our applications ready and able to support our programmatic mission at the time they are needed.

Other definition:

Availability is associated with information where the loss of the information would cause serious problems, either because it would be costly to replace the information or because it would be difficult to function without the information. Thus availability involves both the dollar value and time value. (EPA Information Security Manual, Section 1, "General Information. ")

Benefit-cost analysis

OSWER Core Concept:

Benefit-cost analysis is a systematic approach for comparing alternative ways to satisfy an objective. Benefit-cost analyses are conducted throughout the OSWER life cycle. The benefits to be realized through RISK reduction as well as the costs to develop, acquire, implement, operate, periodically evaluate and eventually archive SECURITY MEASURES need to be considered along with all other application benefits and costs.

Computer Application

Other definition:

The use for which a system is intentionally employed (NBS-500-109; page 3 quote from FIPS 102, "Guideline for Computer Security Certification and Accreditation. ")

Synonym: application(s)

Computer System

Other definition:

An assembly of elements including at least hardware and usually also software, data, procedures, and people, so related as to behave as an interacting or interdependent unity (NBS-500-109; page 3 quote from FIPS 102, "Guideline for Computer Security Certification and Accreditation. ")

Synonym: system(s)

Confidentiality

OSWER Core Concept:

Some OSWER applications contain data or provide information which during a specified period of time is not subject to the Freedom of Information Act and must not be disclosed without authorization. *CONFIDENTIALITY* refers to our need to have certain of our data and information held in confidence.

Other definition:

Information where disclosure would be undesirable or unlawful. (EPA Information Security Manual, Section 1, "General Information. ")

Information Resource

OSWER Core Concept:

Every OSWER application involves data, information, hardware, software, documentation, facilities, telecommunications and trained staff. These components of each application are our *INFORMATION RESOURCES*. All *INFORMATION RESOURCES* have value in and of themselves. Equipment costs money to acquire, replace or repair. Staff costs money to hire, retain and train. Software costs money to develop and maintain. However, the ultimate value of our *INFORMATION RESOURCES* are the support they provide to our programmatic mission.

Synonym: Asset, Information Asset
("EPA Information Security Manual")

Integrity

OSWER Core Concept:

All *INFORMATION RESOURCE* components of an application must retain the functionality they were designed to have in order to support the programmatic mission. *INFORMATION RESOURCES* have *INTEGRITY* as long as their functionality remains uncompromised; that is, they must do no more, no less than their intended purpose.

Other definition:

Information or applications where accuracy and reliability are of particular concern. In short, integrity is concerned with protecting information from corruption. (EPA Information Security Manual, Section 1, "General Information. ")

Risk

OSWER Core Concept:

Technically, *RISK*, also termed "loss expectancy," is the predicted loss from an *ADVERSE EVENT* during a certain period of time. *RISK* is often expressed in terms of dollars and cents, but not always. The period of time is usually expressed in years, but not necessarily so. For example, the *RISK* of having to reenter transactions which were lost due to hardware failure could be $5 per update cycle. The *RISK* of having to pay prompt payment penalties due to a software error in an accounts payable program could be $25,000 per year. Non-monetary *RISKS* are sometimes expressed in terms such as inconvenience, delay and loss of credibility.

Other definition:

Risk is the probability that an asset will be lost due to a vulnerability in dollars or time units. (Computer and Communications Security, Strategies for the 1990's, James Cooper.)

Risk Analysis

OSWER Core Concept:

The methodology to determine *RISK* by analyzing potential *ADVERSE EVENTS*, *THREATS*, and *VULNERABILITIES* against *INFORMATION RESOURCES*, as well as the likelihood of occurrence, is called *RISK ANALYSIS*. *RISK ANALYSES* are

either qualitative or quantitative. They may be conducted at a very summary level, in great detail, or somewhere in between.

Other definition:

Risk Analysis is a means of measuring and assessing the relative vulnerabilities and threats to a collection of sensitive data and the people, systems, and installations involved in storing and processing that data. Its purpose is to determine how security measures can be effectively applied to minimize potential loss. Risk analyses may vary from an informal, qualitative review of microcomputer installation to a formal, fully quantified review of a major computer center. (EPA Information Security Manual, Appendix A, "Information Security. ")

Security Measure

OSWER Core Concept:

SECURITY MEASURES counter or control *THREATS*. and are categorized by their purpose (prevention, detection, minimization and recovery) and by general type (physical, technical, administrative, and managerial).

Synonym: **Safeguard, Control**
("EPA Information Security Manual")

Sensitivity/Sensitive

OSWER Core Concept:

All OSWER applications are *SENSITIVE* to some degree. This is because, to some extent, they are *VULNERABLE* to loss of *AVAILABILITY* and/or *INTEGRITY*, to *INAPPROPRIATE USE* and some to loss of *CONFIDENTIALITY*. However, there are different degrees of *SENSITIVITY* depending on the relevance of OSWER's *SECURITY OBJECTIVES* to the information management problem to be solved. For example, *AVAILABILITY* might be very relevant to a mission critical application; *INTEGRITY* to a decision support application, and *CONFIDENTIALITY* to an application processing confidential business information. It follows that the greater the relevancy, the greater the degree of *SENSITIVITY*.

Other definition:

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal

programs, or the privacy to which individuals are entitled under the Privacy Act but which has not been specifically authorized under criteria established by an executive order or an Act of Congress to be kept secret in the interest of National Defense or foreign policy. ("Computer Security Act of 1987," PL100-235.)

Other definition:

Information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction of the information. For the purposes of this program, information is categorized as being sensitive or not sensitive. Because sensitivity is a matter of degree, certain sensitive information is further defined as being "highly" sensitive. Highly sensitive information whose loss would seriously affect the Agency's ability to function, threaten the national security or jeopardize human life and welfare. Specifically, information of this type includes National Security Information, information critical to the performance of a primary agency mission, information that is life critical and financial information related to check issuance, funds transfer and similar asset accounting/control functions. Other sensitive is information whose loss would acutely embarrass the agency, subject the agency to litigation or impair the long-run ability of the agency to fulfill its mission. Information of this type includes Privacy Act information, Confidential Business Information, enforcement confidential information, information that the Freedom of Information Act exempts from disclosure, budgetary data prior to release by OMB and information of high value to the agency or a particular organization. (EPA Information Security Manual, Appendix A, "Information Security. ")

Threat

OSWER Core Concept:

A *THREAT* is anything that can cause an *ADVERSE EVENT*. Every application is faced with countless *THREATS*. For the sake of simplicity, however, they can be thought of as just two basic types: people and change to the environment. People can deliberately or inadvertently cause *ADVERSE EVENTS*. *THREATS* can be as obvious as an earthquake or as subtle as a virus. They can change throughout an application's *life cycle*, and frequently do so.

Vulnerability

OSWER Core Concept:

Where there is a chance that a *THREAT* can reach an *INFORMATION RESOURCE* and cause an *ADVERSE EVENT* there is *VULNERABILITY*. Identifying and communicating *VULNERABILITY* can be quite challenging. While some *VULNERABILITIES* are immediately obvious (i.e., a password posted on the wall), others may be much more technical or subtle (i.e., spaghetti code). In general, you can assume that the more complex, distributed, and widely used your application is, the more *VULNERABLE* it is.

Appendix B: Reference Materials

The following documents and reference materials were used to prepare this practice paper. The Information Management Staff (IMS) in the Office of Solid Waste and Emergency Response (OSWER) would like to thank each of the authors for their contributions toward the development of the Computer Application Security Management Practice Paper. The EPA Headquarters Library and the Washington Information Center were integral to the development of this paper and also deserve recognition.

Documentation

Appendix B includes a summary of documents most currently applicable to the management, security, and control of computer applications in the Federal Government and is divided into the following categories:

- Laws
- OMB Circulars and Bulletins
- Special Publications and Guidelines
- Federal Information Processing Standards (FIPS)
- OSWER System Life Cycle Management Guidance (SLCMG)
- Other Related Documents

Laws

Privacy Act of 1974 (Public Law 93-579). The Privacy Act of 1974 protects information related to individuals that is maintained in Federal information systems. The Act establishes specific criteria for maintaining the confidentiality of sensitive data and guidelines for determining which data are covered by the Act. Under the Act Federal agencies and employees are responsible for:

- Maintaining the confidentiality of data covered by the Act, and
- Taking those actions necessary to reasonable ensure that data (concerning individuals) maintained in Federal information systems are accurate. Failure to comply with these provisions can result in criminal and civil penalties for both the agency and the employees of the agency found liable.

Electronic Communications Privacy Act of 1986 (Public Law 99-508). This legislation establishes specific protections that update wiretap and privacy statutes to make them more effective relative to advancements in technology. The legislation protects remote computer services, electronic mail, cellular telephones conversations, satellite transmissions, and other telecommunications technologies. The law also establishes clear guidelines that must be met by Government officials prior to requiring a remote processing services company to provide information from a customer file.

The Computer Security Act of 1987(Public Law 100-235). This law specifies provisions related to the protection of computer-related assets (hardware, software, and data) which include:

- Assignment of responsibility for the development of computer security guidelines and standards to the NIST.
- Requirement that Federal agencies identify existing systems and systems under development which contain sensitive information.
- Requirement for development of a security plan for each identified sensitive computer system within one year of enactment of the Act.
- Requirement for mandatory, periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of Federal computer systems.

OMB Circulars and Bulletins

Office of Management and Budget (OMB) Circular A-71: Security of Federal Automated Information Systems established that financial information should be considered sensitive.

Office of Management and Budget (OMB) Circular A-123: Internal Control Systems established that protection requirements exist for all internal control information. Guidelines for conducting internal controls and preparing an accreditation statement is provided.

Office of Management and Budget (OMB) Circular A-130: Management of Federal Information Resources revises and consolidates Federal policy for the management of Federal information resources by:

- Recognizing that information itself is a valuable national asset that must by managed and protected; and

- Expanding the definition of security to include the appropriate functioning of systems (i.e., systems must do exactly what they are supposed to do and nothing more) as well as the protection of information that is within the systems.

Office of Management and Budget (OMB) Bulletin 90-08: Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information established guidance for activities required by the Computer Security Act of 1987.

Special Publications and Guidelines

U. S. Department of Commerce, National Bureau of Standards, Computer Science and Technology, Security of Personal Computer Systems: A Management Guide, NBS Special Publication 500-120, January, 1985. Provides information on types of security controls which can be used to ensure the security of personal computer systems.

U. S. Department of Commerce, National Bureau of Standards, Guide on Selecting ADP Backup Process Alternatives, NBS Special Publication 500-134, 1985. Provides managers and others responsible for developing automatic data processing (ADP) contingency plans with an approach for selecting an alternative data processing capability. A checklist for evaluating the suitability of the alternative is provided.

U. S. Department of Commerce, National Bureau of Standards, Overview of Computer Security Certification and Accreditation, NBS Special Publication 500-109, April, 1984. Provides ADP policy managers, information resource managers, ADP technical managers, and ADP staff with a comprehensive summary of and guide to FIPS PUB 102, "Guideline to Computer Security Certification and Accreditation," September 27, 1983.

Federal Information Processing Standards (FIPS) Publications

The following descriptions were extracted from the "Federal Information Processing Standards Publications Index," February, 1988.

U. S. Department of Commerce, Guidelines for Security of Computer Applications, NBS Standard Publication 73, Institute for Computer Sciences and Technology, Federal Information Processing Standards Publication 73: June 1980. Describes the different security objectives for a computer application, explains the control

measures that can be used, and identifies the decisions that should be made at each stage in the life cycle of a sensitive computer application.

U. S. Department of Commerce, Guidelines for Computer Security Certification and Accreditation, Institute for Computer Sciences and Technology, Federal Information Processing Standards Publication 102: 1983. Presents a detailed approach to developing a program and performing a technical process for certifying and accrediting sensitive applications.

U. S. Department of Commerce, Guideline for Automatic Data Processing Risk Analysis, NBS Standard Publication 65, Institute for Computer Sciences and Technology, Federal Information Processing Standards Publications 65: August 1979. Presents a technique for conducting a risk analysis of an ADP facility and related assets.

U. S. Department of Commerce, Guideline for ADP Contingency Planning, NBS Standard Publication 87, Institute for Computer Sciences and Technology, Federal Information Processing Standards Publication 87: March 1981. Describes what should be considered when developing a contingency plan for an ADP facility. Provides a suggested structure and format which may be used as a starting point from which to design a plan to fit each specific operation.

OSWER System Life Cycle Management Guidance

U. S. Environmental Protection Agency, Office of Solid Waste and Emergency Response, System Life Cycle Management Guidance, Directive #9028. 00, July, 1988. Provides EPA project managers with details concerning their responsibilities under the OSWER System Life Cycle Management Guidance (SLCMG).

U. S. Environmental Protection Agency, Office of Solid Waste and Emergency Response, Practice Paper: Data Management During the System Life Cycle, Directive #9028. 00a, January, 1989. Provides EPA project managers with details concerning their responsibilities for data management under the OSWER System Life Cycle Management Guidance (SLCMG).

U. S. Environmental Protection Agency, Office of Solid Waste and Emergency Response, Practice Paper: Project Management Plan, Directive #9028. 00a, January, 1989. Describes the structure and content of the Project Management Plan, a key document of the OSWER System Life Cycle Management Guidance, and its evolution through the system life cycle.

U. S. Environmental Protection Agency, Office of Solid Waste and Emergency Response, Practice Paper: Configuration Management, Directive #9028. 00a, January, 1989. Describes OSWER's practice of configuration management, tailoring industry proven configuration management methods and techniques to the OSWER environment.

U. S. Environmental Protection Agency, Office of Solid Waste and Emergency Response, Practice Paper: Benefit- Cost Analysis, Directive #9028. 00a, January, 1989. Presents the benefit-cost analysis noted in the OSWER System Life Cycle Management Guidance Parts 1 and 2 in the context of the OSWER program and information management environment. This paper also complements Chapter 3: Options Analysis, of the EPA Systems Design and Development Guidance, Volume B, issued by the Office of Information Resources Management.

Other Related Documents

Cooper, James Arlin, Computer & Communications Security, Strategies for the 1990's, 1989. Devotes most of its chapters to six aspects of security: physical protection, personnel considerations, legal and regulatory aspects, hardware security, software security, and network security. The last chapter of the book does an excellent job of presenting a consolidated global approach with projections for the future of computer and communications security in the 1990's.

U. S. Department of Energy , DOE Risk Assessment Guideline, A Structured Approach, Office of ADP Management: DOE/MA-0356 April, 1989. Provides DOE with a 6 step approach for conducting a risk analysis with each step focusing on a particular area of concern. Worksheets provide the necessary data sets and an organized format to address each of the areas of concern.

U. S. Environmental Protection Agency, Automated Laboratory Standards: Evaluation of the Standards and Procedures Used In Automated Clinical Laboratories, Office of Information Resources Management, May, 1990. Describes the findings of a review of standards and practices used in existing automated systems in a limited number of laboratories in a clinical setting under the assumption that these laboratories generate data of high integrity.

U. S. Environmental Protection Agency, Automated Laboratory Standards: Evaluation of Good Laboratory Practices for EPA Programs, Office of Information Resources Management, June, 1990. Describes the findings of a review of existing Good Laboratory Practices (GLPs) as well as the impact of those standards on automated laboratory practices. EPA's GLPs are regulations that describe

acceptable laboratory management practices to ensure the quality and integrity of health, environmental, and chemical data submitted to the Agency are met.

U. S Environmental Protection Agency, Office of Information Resources Management, EPA Information Security Manual, December, 1989. Establishes security procedures for safeguarding Agency information resources and provides overall guidance to EPA managers and staff in implementing those procedures.

U. S Environmental Protection Agency, Office of Information Resources Management, EPA Information Security Manual For Personal Computers, December, 1989. Establishes security procedures for safeguarding Agency personal computers and provides overall guidance to EPA managers and staff in implementing those procedures.

U. S. Executive Office of the President, Office of Management and Budget, Model Framework for Management Control Over Automated Information Systems, January , 1988. Focuses heavily on the system life cycle as a means of management control.

U. S. General Services Administration, Federal Systems Integration and Management Center, Office of Technical Assistance, Information Technology Installation Security, December, 1988. Written as guide to assist agencies in establishing and maintaining a security program to protect unclassified information handled at Government information technology installations.

U.S. Small Business Administration, Office of Business Development, A Small Business Guide to Computer Security, April, 1987. Contains a detailed self-audit checklist that is useful for smaller systems security management.

Videos

The EPA Headquarters Library has the following computer/information security video tapes available for check-out:

- "Data Security: BE AWARE or BEWARE"
- "Computer System Security: Access Control"
- "Computer System Security: Access - The Ins and Outs"
- "Information Security: Protecting Our Major Asset"

- "Computer System Security: Access - The Ins and Outs"
- "Information Security: Protecting Our Major Asset"

* After a review within OSWER, this video will be shown in October during a series of "brown bag" lunch sessions as part of the OSWER Security Program.

The Washington Information Center (WIC) has a selection of videos available for check-out through their products and services contract with Applied Learning. Applied Learning is a company in the business of providing training needs to technology-based organizations. The following list is a sample of their selection:

- "System Security Design Techniques"
- "Computer Security Techniques"
- "Security Training"
- "RACF Workshop Computer Security Overview"
- "Security in Micro-to-Mainframe Links"
- "VAX/VMS System Security"
- "Controlling Information Systems"
- "Corporate Computer Security Strategy"
- "EDP Quality Assurance: A Management Overview"

Appendix C: Security Characterization Matrices

Key to the development of an application security management *approach* and its evolution through the OSWER *life cycle* is a thorough understanding of:

- Types of *INFORMATION RESOURCES*
- Typical *ADVERSE EVENTS* that may affect each type of *INFORMATION RESOURCE*
- Potential *THREATS*
- Typical *VULNERABILITIES* that might compromise each type of *INFORMATION RESOURCE* and allow a *THREAT* to cause an *ADVERSE EVENT*
- *SECURITY MEASURES* available to counter *THREATS*

This appendix provides detailed examples, in matrix format, showing how each of these might be characterized and evaluated during the *Initiation phase, Concept phase,* and *Definition stage* of the OSWER *life cycle.*

INFORMATION RESOURCES are categorized as follows:

- Data
- Information
- Hardware
- Software
- Documentation
- Facilities
- Telecommunications
- Trained Staff

The *ADVERSE EVENTS* (shown in Exhibit C-1) and *VULNERABILITIES* (shown in Exhibit C-3) are grouped according to these *INFORMATION RESOURCE* categories.

The *THREATS* (shown in Exhibit C-2) are grouped according to type, as follows:

- *THREATS* from People, both deliberate and inadvertent
- *THREATS* from Change to the Environment, both unexpected and planned

Each individual *ADVERSE EVENT, THREAT,* and *VULNERABILITY* is characterized in three ways:

- Source document
- Applicability to the *SECURITY OBJECTIVES* of *AVAILABILITY, INTEGRITY, CONFIDENTIALITY* , and *APPROPRIATE USE*
- Applicability to each typical processing environment, as defined in the EPA Information Security Manual. In general:
  - Manual systems, or manual components of automated systems, are least *VULNERABLE.*
  - Stand-alone personal computers (PC) and word processors (WP) are slightly more *VULNERABLE.*
  - PCs involved in Local Area Networks (LAN) or remote access terminals for larger systems are more *VULNERABLE,* in general, because of the increased number of users involved and the geographic diversity of node locations.
  - Mainframe (MF) and minicomputer systems are most *VULNERABLE,* in general, because of the large number of users, large number of concurrent applications, and greater complexity of the applications.

Exhibit C-4 provides a detailed characterization for the various types of *SECURITY MEASURES* that are available. The *SECURITY MEASURES* are grouped according to type as follows:

- Physical
- Technical
- Administrative
- Managerial

In the first part of Exhibit C-4, each individual *SECURITY MEASURE* is characterized in four ways:

- Source document
- Level (High, Medium, or Low) of *SENSITIVITY* to the *SECURITY OBJECTIVES* of *AVAILABILITY, INTEGRITY, CONFIDENTIALITY,* and *APPROPRIATE USE.* This level is assigned according to the guidance in the "EPA Information Security Manual. "
- Purpose (Prevention, Detection, Minimization, or Recovery)
- Applicability to each typical processing environment, as above

The second part of Exhibit C-4 shows where and how each *SECURITY MEASURE* is addressed in the OSWER *life cycle,* as follows:

- *Initiation Phase* (Planning)
- *Concept Phase* (Analysis)
- *Definition Stage* (Requirements)
- *Design Stage* (Design)
- *Development Stage* (Code/Test, Construct, or Acquire)
- *Implementation Stage* (Implement)
- *Operation Stage* (Use)
- *Evaluation Stage* (Evaluate)
- *Archive Stage* (Stop)

Further guidance on the use of these materials during the OSWER *life cycle* is provided in Chapter 4. These matrices are designed to be used as a provocative tool rather than as a comprehensive list. They are not to be considered complete or rigid, and are intended to be tailored to fit particular projects.

EXHIBIT C-1: ADVERSE EVENTS CHARACTERIZATION MATRIX

Adverse Events (by Information Resource)	SOURCE	OBJECTIVE				TYPICAL PROCESSING ENVIRONMENT			
		Avail.	Integ.	Confid.	Use	Mini/MF	LAN/Rem.	PC/WP	Manual
Data									
Loss	B	√	√			√	√	√	√
Damage	E		√			√	√	√	√
Inaccuracy	B		√			√	√	√	√
Information									
Loss	F	√	√			√	√	√	√
Disclosure	F			√		√	√	√	√
Inaccuracy	F		√			√	√	√	√
Falsification	F		√	√	√	√	√	√	√
Misuse				√	√	√	√	√	√
Hardware									
Failure	E	√	√			√	√	√	
Malfunction (but not total failure)		√	√	√		√	√	√	
Inability to restart	E	√				√	√	√	
Loss	F	√				√	√	√	
Misuse					√	√	√	√	
Software									
Failure		√	√			√	√	√	
Invalid processing			√	√		√	√	√	
Corruption			√	√		√	√	√	
Loss	F	√				√	√	√	
License Infringement					√	√	√	√	
Misuse				√	√	√	√	√	
Documentation									
Loss		√				√	√	√	√
Inaccuracy			√			√	√	√	√
Disclosure				√		√	√	√	√
Misuse				√	√	√	√	√	

Legend for SOURCE: E = mentioned in EPA Information Security Manual
F = mentioned in FIPS PUB 73
B = both

EXHIBIT C-1: ADVERSE EVENTS CHARACTERIZATION MATRIX

Adverse Events (by Information Resource)	SOURCE	OBJECTIVE				TYPICAL PROCESSING ENVIRONMENT			
		Avail.	Integ.	Confid.	Use	Mini/MF	LAN/Rem.	PC/WP	Manual
Facilities									
Loss		√				√	√	√	√
Damage (reduced capability)		√		√		√	√	√	√
Misuse					√	√	√	√	√
Telecommunications									
Loss		√				√	√		
Garbling		√	√			√	√		
Misuse				√	√	√	√		
Trained Staff									
Loss		√				√	√	√	√
Productivity Decrease		√	√	√	√	√	√	√	√

Legend for SOURCE: E = mentioned in EPA Information Security Manual
F = mentioned in FIPS PUB 73
B = both

EXHIBIT C-2: THREATS CHARACTERIZATION MATRIX

Threats (by Type)	SOURCE	OBJECTIVE				TYPICAL PROCESSING ENVIRONMENT			
		Avail.	Integ.	Confid.	Use	Mini/MF	LAN/Rem.	PC/WP	Manual
Threats from People									
Deliberate Actions									
Disgruntlement									
Fear of computerization		✓	✓			✓	✓	✓	✓
Fear of performance monitoring	E	✓	✓			✓	✓	✓	✓
Fear over potential loss of job	E	✓		✓		✓	✓	✓	✓
Dismissal		✓	✓	✓	✓	✓	✓	✓	✓
Hostility		✓	✓	✓		✓	✓	✓	✓
General dissatisfaction		✓	✓	✓	✓	✓	✓	✓	✓
Maliciousness									
Vandalism		✓				✓	✓	✓	✓
Terrorism		✓				✓	✓	✓	✓
Viruses/pranks/spoofing	B	✓	✓	✓		✓	✓	✓	
Sabotage	E	✓	✓	✓		✓	✓	✓	✓
Greed									
Theft	E	✓		✓	✓	✓	✓	✓	✓
Fraud	E		✓		✓	✓	✓	✓	✓
Embezzlement			✓		✓	✓	✓	✓	✓
Influence actions (e.g., Superfund enforcement)		✓	✓	✓		✓	✓	✓	✓
Misuse of licensed software					✓		✓	✓	
Inadvertent Actions									
Lack of training									
Invalid data entry	F		✓			✓	✓	✓	✓
Accidental modification/loss of data		✓	✓			✓	✓	✓	✓
Incorrect user commands	F	✓	✓			✓	✓	✓	
Misuse of licensed software					✓		✓	✓	
Carelessness									
Erroneous source data	F		✓			✓	✓	✓	✓
Invalid data entry	F		✓			✓	✓	✓	✓
Accidental modification/loss of data		✓		✓		✓	✓	✓	✓
Incorrect user commands	F	✓	✓			✓	✓	✓	✓
Insufficient time to complete task		✓	✓	✓		✓	✓	✓	✓

Legend for SOURCE: E = mentioned in EPA Information Security Manual
F = mentioned in FIPS PUB 73
B = both

EXHIBIT C-2: THREATS CHA. .CTERIZATION MATRIX

Threats (by Type)	SOURCE	OBJECTIVE				TYPICAL PROCESSING ENVIRONMENT			
		Avail.	Integ.	Confid.	Use	Mini/MF	LAN/Rem.	PC/WP	Manual
Threats from Environmental Changes									
Unexpected Changes									
Fire		√		√		√	√	√	√
Flood/water damage		√		√		√	√	√	√
Wind, earthquake, etc.		√		√		√	√	√	√
Debris		√				√	√	√	√
Change in humidity		√				√	√	√	
Change in temperature		√				√	√	√	
Dust		√				√	√	√	
Smoke		√				√	√	√	
Power failure/surge		√	√			√	√	√	
Static		√	√			√	√	√	
Planned Changes									
Periodic maintenance		√		√	√	√	√	√	
Packaged software upgrade		√	√	√		√	√	√	
Custom software upgrade		√	√	√		√	√	√	

Legend for SOURCE: E = mentioned in EPA Information Security Manual
F = mentioned in FIPS PUB 73
B = both

EXHIBIT C-3: VULNERABILITIES CHARACTERIZATION MATRIX

Vulnerabilities (by Information Resource)	SOURCE	OBJECTIVE				TYPICAL PROCESSING ENVIRONMENT			
		Avail.	Integ.	Confid.	Use	Mini/MF	LAN/Rem.	PC/WP	Manual
Data									
Unprotected password		√	√	√	√	√	√	√	
Uncontrolled access or poor authorization process	F	√	√	√	√	√	√	√	√
Non-erasure of temporary or deleted files	E		√	√	√	√	√	√	
Poor backup/recovery practices	E	√	√			√	√	√	
Poor media handling practices	E	√	√	√	√	√	√	√	
Lack of validation			√			√	√	√	√
File handling utilities	E	√	√	√	√	√	√	√	
Information									
Unprotected password			√	√	√	√	√	√	
Uncontrolled access or poor authorization process	F	√	√	√	√	√	√	√	√
Information left on screen			√	√	√	√	√	√	
Unsecured hardcopy	E		√	√	√	√	√	√	√
Improperly marked hardcopy			√	√	√	√	√	√	√
Undestroyed printer/typewriter ribbons	E		√	√		√	√	√	√
Hardware									
Poor maintenance practices		√			√	√	√	√	
Poor testing practices		√	√			√	√	√	
Unprotected password		√	√		√	√	√	√	
Uncontrolled access or poor authorization process		√	√		√	√	√	√	
Software									
Poor design practices		√	√	√		√	√	√	
Poor coding practices		√	√	√		√	√	√	
Poor testing practices		√	√	√		√	√	√	
Poor backup/recovery practices		√	√	√		√	√	√	
Lack of Configuration Management		√	√	√		√	√	√	
Operating System and Utility flaws	F	√	√	√	√	√	√	√	
Bugs in packaged software	F	√	√	√	√	√	√	√	
Uncontrolled access or poor authorization process		√	√	√	√	√	√	√	
Documentation									
Poor technical writing practices			√			√	√	√	√
Poor distribution/update		√	√			√	√	√	√
Lack of Configuration Management		√	√	√	√	√	√	√	√

Legend for SOURCE: E = mentioned in EPA Information Security Manual
F = mentioned in FIPS PUB 73
B = both

EXHIBIT C-3: VULNERABILITIE. HARACTERIZATION MATRIX

Vulnerabilities (by Information Resource)	SOURCE	OBJECTIVE				TYPICAL PROCESSING ENVIRONMENT			
		Avail.	Integ.	Confid.	Use	Mini/MF	LAN/Rem.	PC/WP	Manual
Facilities									
Poor siting		√				√	√		
Poor construction		√				√	√		
Poor maintenance		√			√	√	√	√	√
Poor access control	F	√			√	√	√	√	√
Telecommunications									
Poor maintenance		√				√	√		
Uncontrolled dial-in access	F		√	√	√	√	√		
Uncontrolled LAN/remote access	E		√	√	√	√	√		
Trained Staff									
Lack of training			√	√	√	√	√	√	√
Lack of supervision		√	√	√	√	√	√	√	√
Lack of procedures		√	√	√	√	√	√	√	√
Lack of screening			√	√	√	√	√	√	√

Legend for SOURCE: E = mentioned in EPA Information Security Manual
F = mentioned in FIPS PUB 73
B = both